AGREEMENT EXTENDING AND AMENDING THE SAFE PASSAGE SERVICES AGREEMENT (BRIGHT STAR COMMUNITY)

This Agreement Extending and Amending the Safe Passage Services Agreement ("Extension Agreement") is effective as of this 25th day of May 2021 ("Effective Date") and is entered into by and between the Board of Education of the City of Chicago, a body politic and corporate, commonly known as the Chicago Public Schools (the "Board" or "CPS") and Bright Star Community (the "Provider") with its principal place of business located at 735 East 44th Street, Chicago, IL 60653.

RECITALS

- A. The Board and Provider entered into that certain Agreement for Safe Passage Services ("Original Agreement') for a term commencing on August 1, 2018 and continuing through July 31, 2019 (authorized by Board Report 18-0523-PR22), with the Board having two (2) options to renew for a period of one (1) year each.
- B. The Board exercised its first option to renew the Original Agreement pursuant to that certain Agreement Exercising First Option to Renew ("First Renewal Agreement") for a term commencing August 1, 2019 and continuing through July 31, 2020 (authorized by Board Report 19-0424-PR5).
- C. The Board exercised its second option to renew the Original Agreement pursuant to that certain Agreement Exercising Second Option to Renew ("Second Renewal Agreement") for a term commencing August 1, 2020 and continuing through July 31, 2021 (authorized by Board Report 20-0422-PR8). The Original Agreement, the First Renewal Agreement, and the Second Renewal Agreement shall be referred to collectively herein as the "Existing Agreement".
- D. The Board now desires to extend and amend the Existing Agreement to provide home outreach visits for CPS students who have been absent for an extended period of time and to provide door-to-door neighborhood canvassing services within the City of Chicago. Provider accepts this Extension Agreement on the terms and conditions hereinafter set forth. The Existing Agreement and this Extension Agreement shall be collectively referred to herein as the "Agreement".

NOW THEREFORE, in consideration of the foregoing, which are incorporated into and made a part of this Agreement by this reference, and the mutual covenants contained herein, the parties agree as follows:

- 1. **<u>Definitions</u>**: Any and all capitalized terms contained in this Extension Agreement, and not defined herein, shall have the definition as set forth in the Existing Agreement.
- 2. <u>Extension Term</u>: The Parties agree to extend the Existing Agreement for a term commencing on August 1, 2020 continuing through August 31, 2021 ("Extension Term").
- 3. <u>Services</u>: During the Extension Term, Provider shall provide the additional services set forth in the Supplemental Scope of Services (the "Supplemental Services") attached hereto and incorporated herein as <u>Exhibit A-1</u>. These Supplemental Services shall be provided in addition to those Services set forth and described in **Exhibit A** of the Existing Agreement.
- 4. <u>Compensation</u>: During the Extension Term, the total compensation for the Supplemental Services and Services shall not exceed One Hundred Ninety One Thousand Four Hundred Thirteen Dollars (\$191,413.00) ("Maximum Compensation Amount").

It is understood and agreed that the Maximum Compensation Amount is a 'not-to-exceed amount' and is not a guaranteed payment. Compensation shall be based on actual Supplemental Services performed

during the Extension Term, and the Board shall not be obligated to pay for any Services or other deliverables not in compliance with this Agreement. No expenses shall be reimbursed under this Agreement. In the event the Agreement is terminated early, the Board shall only be obligated to pay the fees incurred up to the effective date of termination and Provider shall promptly refund to the Board any payments received from Supplemental Services and deliverables not provided.

5. <u>Confidential Information:</u> Section 8 of the Original Agreement is hereby deleted in its entirety and replaced with the following:

8. Confidential Information; Dissemination of Information; Ownership; Injunctive Relief; Survival:

- **8.1 Confidential Information:** In the performance of the Agreement, Provider may have access to or receive certain information that is not generally known to others ("**Confidential Information**"). Such Confidential Information may include but is not limited to: Student Data, as further defined below, employee data, technical data or specifications, software, ideas, budget figures, operational details, security details, unpublished school information, CPS financial information, and CPS business plans. It is understood and agreed that Confidential Information also includes proprietary or confidential information of third parties provided by the Board to Provider. Confidential Information will not include information that is: (i) or becomes part of the public domain through no fault of Provider; (ii) made available to Provider by an independent third party having the legal right to make such disclosure; and (iii) information that can be established and documented by Provider to have been independently developed or obtained by Provider without violating the confidentiality obligations of this Agreement and any other agreements with the Board.
- **8.2 Student Data**: Student Data means any data, metadata, information, or other materials of any nature recorded in any form whatsoever, that is generated, disclosed, transmitted, created, or provided by the Board, either directly or through its students, employees, agents, and subcontractors, and all information used, created, or generated through the use of any technology including but not limited to any software, by the Board, through its employees, agents, subcontractors, or the parent or legal guardian of any CPS student, that is directly related to a CPS student. For purposes of this Agreement, Student Data shall still be considered Confidential Information; additional requirements regarding Student Data specifically are described below.
- **8.3** Use of Confidential Information: Provider shall only use Confidential Information for the sole purpose of providing the Services to the Board hereunder and shall not disclose the Confidential Information except to those of its officers, agents, employees, and subcontractors who have a need to access the Confidential Information for the performance of the obligations set forth in this Agreement. Provider shall not copy or reproduce in any manner whatsoever the Confidential Information of the Board without the <u>prior written consent</u> of the Board, except where required for its own internal use in accordance with this Agreement. Provider shall use at least the same standard of care in the protection of Confidential Information as Provider uses to protect its own confidential information, but in any event, such Confidential Information shall be protected in at least a commercially reasonable manner. Notwithstanding the foregoing, it is understood and agreed that such protection of Confidential Information may be subject to the special requirements of the Family Educational Rights and Privacy Act ("FERPA"), the Student Online Personal Protection Act ("SOPPA"), and the Illinois School Student Records Act ("ISSRA") as described in the Compliance with Laws Section.
- 8.4 **De-Identified Data:** De-identified Data will have all direct and indirect personal identifiers removed. This includes, but is not limited to, persistent unique identifiers, name, ID numbers, date of birth, demographic information, location information, and school ID. Provider agrees not to attempt to re-identify de-identified Data. For the purposes of this Agreement, De-

Identified Data will still be considered Confidential Information and treated as such unless expressly provided otherwise in this Agreement.

- 8.5 **Handling of Confidential Information:** Provider shall protect against the unauthorized access, use or disclosure of Confidential Information by employing security measures that are no less protective as those used to protect Provider's own confidential information. When handling Confidential Information, which may include but is not limited to student data, Provider shall:
 - A. When mailing physical copies of Confidential Information, send the Confidential Information in a tamper-proof, labeled container, with a tracking number and a delivery confirmation receipt;
 - B. Not store any Confidential Information on portable or removable electronic media, such as CDs, DVDs, electronic tape, flash drives, etc.;
 - C. Not leave Confidential Information in any medium unsecured and unattended at any time;
 - D. Keep all physical copies (paper, portable or removable electronic media, or other physical representations) of Confidential Information under lock and key, or otherwise have sufficient physical access control measures to prevent unauthorized access;
 - E. Password protect any laptop or other electronic device that contains Confidential Information. Additionally, any laptop or other electronic device that contains Confidential Information shall have its full hard drive encrypted with an encryption key of no less than 256 bits. Provider shall not leave any laptop or other electronic device unattended without enabling a screen-lock or otherwise blocking access to the laptop or other electronic device. Provider shall ensure that no password or other information sufficient to access a laptop or electronic device containing Confidential Information is attached to or located near the laptop or other electronic device at any time.
 - F. Secure the Confidential Information stored on its systems, including but not limited to any servers, by employing adequate security measures to prevent unauthorized access, disclosure and use of that information. These measures include appropriate administrative, physical, and technical safeguards, policies and procedures relating to data access controls. All Confidential Information must be secured in transit using secure FTP services or https/TLS 1.0+. Provider must maintain industry recognized security practices to establish secure application(s), network, and infrastructure architectures.
 - G. Ensure that the manner in which Confidential Information is collected, accessed, used, stored, processed, disposed of and disclosed within Provider's Products, Services, and supporting enterprise complies with applicable data protection and privacy laws, as well as the terms and conditions of this Agreement.
 - H. Conduct periodic risk assessments and remediate any identified security vulnerabilities in a timely manner. Provider will also have a written incident response plan, to include prompt notification of the Board in the event of a security or privacy incident, as well as best practices for responding to a breach of Confidential Information security practices. Provider agrees to share its incident response plan upon request.
 - I. Ensure that its systems and Services include at least the following safeguards:
 - 1. Include component and system level fault tolerance and redundancy in system design.

- 2. Encrypt user passwords in any data storage location and obfuscate password entry fields in any entry interface controlled by the discloser.
- Encrypt Confidential Information at-rest and in-transit.
- 4. Authentication of users at login with a 256-bit or higher encryption algorithm.
- 5. Secure transmission of login credentials.
- 6. Automatic password change routine.
- 7. Trace user system access via a combination of system logs and Google Analytics.
- 8. Secure (encrypt) the audit trails and system generated logs and ensure that they are stored in locations that are inaccessible to automated content discovery software.
- 9. Conduct or undergo system level testing whenever new functionalities are added to the system to reconfirm system security measures are retained and functional, and that interaction with the Board systems is not degraded or compromised.
- 10. Employ an in-line intrusion protection system that inspects incoming data transmissions.
- 11. Prevention of hostile or unauthorized intrusion.
- 12. Backup of all Confidential Information at least once every twenty-four (24) hours. Perform content snapshots at least daily and retain for at least ninety (90) days.
- J. Confidential Information shall be stored, backed up, and served only on servers located in the continental United States. Provider's network where Confidential Information may be stored shall have an in-line intrusion prevention system that inspects incoming data transmissions. Provider shall have a documented disaster recovery plan for the electronic systems where Confidential Information may be stored. Data stored in cloud-based systems must be protected in the same manner as local data as described throughout the Agreement.
- **8.6 Dissemination of Information:** Provider shall not disseminate any Confidential Information to a third party without the prior written consent of the Board. If Provider is presented with a request for documents by any administrative agency or with a *subpoena duces tecum* regarding any Confidential Information which may be in Provider's possession as a result of Services and/or materials provided under the Agreement, Provider shall immediately give notice to the Board and its General Counsel with the understanding that the Board shall have the opportunity to contest such process by any means available to it prior to submission of any documents to a court or other third party. Provider shall not be obligated to withhold delivery of documents beyond the time ordered by a court of law or administrative agency, unless the request for production or subpoena is quashed or withdrawn, or the time to produce is otherwise extended.
- 8.7 **Press Release; Publicity**: Provider shall not issue publicity news releases, grant press interviews, or use any Confidential Information or Board intellectual property (as defined below), including but not limited to the CPS logo or the logos of any schools, during or after the performance of Services without the prior written consent of the authorized representatives of the Board. Furthermore, Provider may not photograph or film or cause others to photograph or film within any CPS school or facility without the prior express written consent of the Board's Chief Communications Officer or his/her designee.
- 8.8 Unauthorized Access, Use, or Disclosure of Confidential Information: If Provider becomes aware of any unauthorized access, use, or disclosure of the Confidential Information, it shall: (i) notify the Board immediately, which shall be no more than twenty-four hours from Provider receiving notice of the unauthorized access, use or disclosure of the Confidential

Information; (ii) take prompt and appropriate action to prevent further unauthorized access, use or disclosure of the Confidential Information; (iii) cooperate with the Board and any government authorities with respect to the investigation and mitigation of any such unauthorized access, use, or disclosure, including the discharge of the Board's duties under the laws; and (iv) take such other actions as the Board may reasonably require to remedy such unauthorized access, use and disclosure, including if required under any federal or state law, providing notification to the affected persons. Provider shall bear the losses and expenses (including attorneys' fees) associated with the breach of its obligations concerning the handling and protection of Confidential Information, including without limitation any costs: (1) of providing notices of a data breach to affected persons and to regulatory bodies; and (2) of remedying and otherwise mitigating any potential damages or harm of the data breach, including without limitation, establishing call centers and providing credit monitoring or credit restoration services, as requested by the Board.

- 8.9 Additional Obligations Regarding Treatment of Student Data: In addition to the above stated obligations for the treatment and handling of Confidential Information, Provider shall abide by the following obligations with regards to any Student Data Provider may receive, store, transmit, handle or otherwise have access to pursuant to this Agreement:
 - A. <u>Student Data Use:</u> Provider shall not use Student Data, including persistent unique identifiers, data created or gathered by Provider's site, Services, and technology, for any purpose, including but not limited to amassing a profile about a CPS student or otherwise identify a CPS student except in furtherance of specific Services as set forth in this Agreement. Provider will use Student Data only for the purpose of fulfilling its duties and delivering Services under this Agreement, and for improving Services under this Agreement in a way that does not otherwise violate the terms of this Agreement regarding the treatment of Confidential Information.
 - B. <u>Student Data Collection:</u> Provider will collect only Student Data necessary to fulfill its duties as outlined in this Agreement.
 - C. <u>Marketing and Advertising:</u> Provider shall not advertise or market to students or their parents/legal guardians when the advertising is based upon any Student Data that Provider has acquired because of the use of that Provider's Services or the use of technology as part of the Services.
 - D. <u>Student Data Mining:</u> Provider is prohibited from mining Student Data. Student Data mining or scanning of user content for the purpose of advertising or marketing to students or their parents is prohibited.
 - E. <u>Student Data Transfer or Destruction:</u> Provider will ensure that all Student Data in its possession and in the possession of any subcontractors, or agents to whom Provider may have transferred Student Data, are destroyed or transferred to the Board under the direction of the Board when Student Data is no longer needed for its specified purpose.
 - F. Rights in and to Student Data: Parties agree that all rights, including all intellectual property rights, associated with such Student Data shall remain the exclusive property of the Board. Nothing in this Agreement is meant and nothing shall be interpreted to mean that the Board releases any ownership or control of Student Data during the performance of the Services under this Agreement. Student Data shall remain under the control of the Board throughout the Term of this Agreement, including any Renewal Terms. This Agreement does not give Provider any rights, implied or otherwise, to Student Data, content, or intellectual property. Provider does not have the right to sell or trade Student Data.

- G. <u>Sale of Student Data:</u> Provider is prohibited from selling, trading, or otherwise transferring Student Data.
- H. <u>Access:</u> Any Student Data held by Provider will be made available to the Board upon request of the Board. The identity of all persons having access to Student Data through Provider will be documented and access will be logged.
- 6. <u>Freedom of Information Act</u>: Provider acknowledges that this Extension Agreement and all documents submitted to the Board related to this contract award are a matter of public record and are subject to the Illinois Freedom of Information Act (5 ILCS 140/1), subject to any permitted exceptions asserted by Provider, and any other comparable state and federal laws and that this Extension Agreement is subject to reporting requirements under 105 ILCS 5/10-20.44. Provider further acknowledges that this Extension Agreement shall be posted on the Board's website at www.cps.edu.
- 7. <u>Agreement</u>: Except as expressly provided in this Extension Agreement, all terms and conditions of the Existing Agreement shall remain in full force and effect during the Extension Term.
- 8. <u>Counterparts and Electronic Signature</u>: This Extension Agreement may be executed in any number of counterparts, each of which shall be deemed to be an original, but all of which together shall constitute but one document. A signature delivered by facsimile or other electronic means shall be considered binding on both parties.

.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK

IN WITNESS WHEREOF, the parties have signed this Extension Agreement as of the date first written above.

BOARD OF EDUCATION OF THE CITY OF CHICAGO		BRIGHT STAR COMMUNITY
By: Jonathan Maples Jonathan Waples Chief Procurement Officer	Ξ	By: Nichola Carter Name: Nichole Carter Title: Chief Program Officer
June 10, 2021 Date: Authority: 21-0428-RS2		Date: 5.28.2021
Approved as to Legal Form: Solution	L B	

Attachments

Exhibit A-1: Supplemental Scope of Services

Exhibit A-1 Supplemental Scope of Services

Board Project Manager: Molly Burke E-Mail: meburke@cps.edu

Board Designee: Adrian Seguara E-Mail:asegura7@cps.edu

Provider's Project Manager: Nicole Carter E-Mail: nichole@brightstarcommunityoutreach.com

Extension Term: August 1, 2020- August 31, 2021

This Supplemental Scope of Services will be conducted pursuant to the terms and conditions of that Agreement by and between Bright Star Community ("**Provider**"), and the Board of Education of the City of Chicago (the "**Board**"), commonly known as the Chicago Public Schools ("**CPS**"). Defined terms used in this Supplemental Scope of Services will have the same meanings as those ascribed to such terms in the Agreement. If there is any conflict between this Supplemental Scope of Services and the Agreement, the Agreement shall govern and control.

I. Overview of Services

Under this Agreement, Provider will provide the "Supplemental Services" described below through its "At Home Ambassador's Program" ("Program"). The goal of the Program is to ensure students who are identified by CPS as students most disengaged from school during remote learning are enrolled in school. Provider will provide Supplemental Services based on need in specific communities and schools identified by CPS.

Provider will dedicate a group of "Home Outreach Ambassadors" to conduct checks at the residences of select CPS students who have been absent from school for an extended period of time and to provide door-to-door neighborhood canvassing services within the City of Chicago. A list of students selected to receive Supplemental Services from Provider will be provided to Vendor by CPS staff from either the selected students' school or from CPS Central Office or via the CPS Aspen system.

Home Outreach Ambassadors Supplemental Services will include, but are not limited to the following: conducting visits to the residences of select CPS students, administering Board-approved surveys or questionnaires to students or other persons residing in the home to discover any potential student safety or engagement concerns, and robust door-to-door canvassing as trusted messengers to share Board approved information about CPS summer programming and the start of the SY21-22 school year. Home Outreach Ambassadors doing either home visits or door-to-door canvassing will be required to deliver the aforementioned information successfully, including in areas where bi-lingual canvassing will be necessary. Home Outreach Ambassadors serving in this capacity must be able to travel to addresses provided for student home visits and/or student canvassing. The Home Outreach Ambassadors will be given a CPS issued electronic tablet for use recording outreach outcomes and information gathered while conducting home visits.

II. Protocols

When conducting all Supplemental Services, Provider and its Home Outreach Ambassadors must abide by the following protocols:

A. Remaining in compliance with all applicable federal, state, county, and municipal, statutes, laws, ordinances, regulations, and guidelines, as well as any Board guidelines, policies, and rules in effect now or later, and as amended from time to time related to COVID-19. Provider shall further comply with evolving requirements to protect the health and safety of all persons that Provider

provides Supplemental Services to as expressed in local, and state guidance from various government agencies. This includes, but is not limited to, adhering to all health and safety guidelines issued by CPS, IDPH, and CDPH related to COVID-19. Provider acknowledges these health and safety guidelines are subject to change. Provider and all Home Outreach Ambassadors must wear Personal Protective Equipment ("**PPE**") and maintain an adequate social distance of at least six feet outdoors. Provider and all Home Outreach Ambassadors must also remain in compliance with all State and City guidelines that are in place at the time Supplemental Services are provided.

- B. Provider and all its Home Outreach Ambassadors will work based on lists of students from both central office and with school based student engagement teams (i.e., principal, counselors, etc) to create a narrative that would be best practice for messaging to the family and getting information to improve student success. Home visits will seek to understand challenges to school engagement and enroll students in summer programming. Home Outreach Ambassadors will serve as conduit between the families and the schools.
- C. When conducting home visits, if the student who is the subject of the home visit is under the age of 18, the Home Outreach Ambassadors will only speak to the student's parents and or guardians, If the student who is the subject of the home visit is under that age of 18 and answers the door and a parent or guardian is not available to speak with the Home Outreach Ambassador, the Home Outreach Ambassadors shall leave the premises of the residence and attempt contact again in the presence of the parent or guardian. In the event that a parent or guardian is not available to speak with the Home Outreach Ambassadors, the Home Outreach Ambassadors may only speak to the student who is the subject of the home visit if that student is over the age of 18 and has the capacity to consent.
- D. During the home visits, Home Outreach Ambassadors shall wear Provider issued identification badges and vests. These vests shall not be yellow.
- E. During home visits, if a Home Outreach Ambassador suspects an emergency situation exists, the ambassador must call 911 and inform the school/program the student attends immediately of the emergency situation. Provider must ensure Home Outreach Ambassadors are aware of this responsibility. It is critical that Home Outreach Ambassador respond to emergency situations in a timely manner.

III. Requirements

While providing the Supplemental Services, Provider shall meet the below requirements:

- A. Have consistent, punctual and good attendance when providing all Supplemental Services;
- B. Be outgoing and adept at relationship building;
- C. Be alert with an attention to identifying situations that may become serious incidents if not addressed;
- D. Have the ability to de-escalate situations that may become serious incidents if not addressed; and
- E. Possess communication skills including verbal skills and ability to write and/or present have access to a working smartphone while conducting home visits

IV. Data

Provider and its Home Outreach Ambassadors shall only have access to the data listed below. All data will only be stored on CPS issued tablets and logged on the CPS tool designated by CPS.

A. CPS will provide Provider and its Home Outreach Ambassadors with lists for the students that require home visits that include the following data: student name, last school attended, age of student, address and recommendation for summer programming.

- B. Provider and its Home Outreach Ambassadors will also collect answers to survey questions about barriers to attendance and school engagement (e.g., transportation issues, child care issues, medical or mental health needs).
- C. Provider and its Home Outreach Ambassadors are prohibited from storing any data on any device other than their CPS issued device. Provider and its Home Outreach Ambassadors shall not store any Student Data on their personal devices under any circumstances
- D. Provider and its Home Outreach Ambassadors shall only utilize the CPS designated tool to record data. The Board's Project Manager or Board's Designee shall inform Provider of the CPS designated tool prior to the commencement of Supplemental Services

V. Obligations While Conducting Home Visits and Outreach Activities

Provider and its Home Outreach Ambassadors will conduct outreach, canvassing activities, and home visits. Provider and its Home Outreach Ambassadors' obligations while conducting such activities will minimally consist of the following obligations:

- A. Home Outreach Ambassador teams will consist of two workers that will work a maximum of five (5) hours per day. The number of days per week that teams will work will be dependent on school needs. The days that Home Outreach Ambassadors will need to perform Supplemental Services will include Saturdays. Home Outreach Ambassador teams will conduct these activities from June 23, 2021 to August 27, 2021. The number of days each Home Outreach Ambassador team must work and the number of Home Outreach Ambassadors teams Provider will be required to provide will be based on the student caseloads in schools covered by Provider. CPS will verify the number of teams and hour requirements with Provider prior to the start of Supplemental Services. Provider must be available to have its Home Outreach Ambassador Teams support more than one school.
- B. Upon request from the Board Designee, Provider will conduct repeated visits to selected homes to develop relationships with students and/or families with the goal of removing barriers to student reengagement. However, Provider and its Home Outreach Ambassadors shall only engage with students if the student is over 18 or if the student is under the age of 18, if the student's parent or guardian is present.
- C. Each Home Outreach Ambassador will be provided with a CPS issued tablet to enter outcomes from the home visits. Provider will designate a Home Outreach Provider. The Home Outreach Provider will be responsible for logging contact attempts and contact outcomes into the CPS Aspen System. Recording all contact attempts; which at minimum will include: a) whether contact was made with student and family during the outreach attempt and b) the results of any surveys the Home Outreach Ambassadors have been asked to conduct.
- D. The Home Outreach Provider will also be responsible for making all home visits assignments based on the student lists it receives from the Board via the CPS Aspen system or from CPS staff.
- E. Follow the guidelines given by CPS regarding key information to convey and information to solicit from students/families during canvassing outreach and home visits (as described above in Section IV: Data).
- F. Record all contact attempts in the designated CPS tool. This tool will be selected by CPS and Provider will be informed by the Board's Project Manager or Designee of which tool shall be utilized. The information regarding contact attempts that Provider will record will include minimally the following: a) whether contact was made with the student's family during the outreach attempt and b) the results of any surveys the Home Outreach Ambassadors have been asked to conduct.

- G. From June 23, 2021 through August 27, 2021, Provider will also provide canvassing services. Canvassers will distribute marketing materials to designated community areas. Canvassing will take place on Mondays, Wednesdays, and Fridays. CPS will provide materials for canvassing which will include door hangers and flyers for back to school marketing efforts.
- H. Submit a weekly report to the Board Designee in the designated CPS tool. CPS will inform Provider of which tool shall be utilized and to process for submitting weekly reports to that tool. Weekly reports will include minimally the number of visits conducted by students, and outcome of the visits, (eq., no contact made, contact made, bad address).

VI. Outcomes:

Provider's services will result in the following:

- A. Increased student enrollment and attendance in summer re-engagement efforts and SY22 enrollment and attendance
- B. Through information collected from outreach visits, a better understanding for CPS regarding why students and families are disengaged, informing how we best address these needs in the fall of 2021.