Flock Safety and The University of Texas at Tyler: Data Transfer Agreement

THIS AGREEMENT effective 1 Nov 2023 ("Effective Date") and continuing through January, 2024 ("Term") is made and entered into by and between Flock Safety, Inc. ("Provider") and the Recipient of the data, The University of Texas at Tyler ("Recipient").

In consideration of the Recipient's promises contained herein, Provider agrees to provide data to the Recipient for the sole purpose of research in the field of public safety technology, and undertaken by the Recipient through Professor Richard Helfers of University of Texas at Tyler, in coordination with Professor Johnny Nhan of Texas Christian University ("Investigator(s)") or person(s) directly under the direction of the Investigators upon the following terms and conditions. Additional data may be provided under amendment to this Agreement that is executed by the party's authorized representatives.

1. The data ("Data") to be furnished to Recipient by Provider will consist of anonymized data related to Provider's customers or such other data and information as Provider furnishes, in its sole discretion, that relates or corresponds to the Research. Customers have consented to Provider's use of the Data for these purposes.

2. The Research ("Research") will consist of a white paper written jointly by Provider and Recipient on the use and efficacy of license plate readers by law enforcement.

3. Provider hereby agrees to provide Data to Recipient and consents to Recipient using and analyzing Data for the Research. Recipient will not use the Data for any purpose other than in fulfillment of the Research. Recipient will not make any commercial use of the Data. Provider will retain the unrestricted right to distribute the Data to other commercial or noncommercial entities and for other purposes.

4. Recipient acknowledges that the Data is the property of Provider and that Provider retains ownership of the Data.

5. The Data is provided AS IS. Provider makes no representations, conditions or warranties, either express or implied with respect to any of the Data. Without limiting the generality of the foregoing, Provider expressly disclaims any implied warranty, condition or representation that the Data corresponds with a particular description, is of merchantable quality or fit for a particular purpose. Recipient will report any systematic problems with the Data to the Provider. Data that has been manipulated or re-processed by either the Provider or Recipient is the responsibility of that Party.

6. Recipient agrees that Data is confidential to Provider and will not transfer or otherwise disclose the Data to, or for the use thereof by, any person except persons in the Investigators' research group for the sole purpose of the Research.

7. Recipient shall immediately notify Provider upon discovery of any disclosure not authorized hereunder and take reasonable steps to prevent any further unauthorized disclosure or

unauthorized use. Recipient shall be responsible for ensuring the confidentiality of Data by Recipient's employees and/or students.

8. Data Security

   a. Recipient shall maintain a comprehensive information security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of Data. At a minimum, the information security program shall include the requirements listed in this Section – Data Security.

   b. Recipient shall provide physical and logical protection for all related hardware, software, applications, and data that meet or exceed industry standards and requirements as set forth in this Agreement. Recipient shall take full responsibility for the security of all Data in its possession, and shall hold Provider harmless for any damages or liabilities resulting from the unauthorized disclosure or loss thereof. Recipient shall provide for the security of Data, in a form acceptable to Provider, including, without limitation, non-disclosure, use of appropriate technology, security practices, computer access security, data access security, data storage encryption, data transmission encryption, security inspections, network firewalls, intrusion detection (host and network), data security logging and monitoring systems, and audits.

   c. Recipient shall provide Provider or its designated representatives with access, subject to Recipient's reasonable access security requirements, for the purpose of inspecting and monitoring access and use of Data and evaluating physical and logical security control effectiveness.

   d. Recipient shall have strong access controls, including role-based access to ensure that only authorized individuals have access to Data.

   e. Workstations and other data processing devices must automatically lock when not in use, and must be manually locked when left unattended.

   f. Recipient shall protect all Data with a complex password. Recipient shall ensure passwords are confidential and prohibit the sharing of passwords. Passwords must not be written down or stored in an unsecure location. Recipient shall periodically change passwords and shall ensure passwords are not reused. Recipient shall have password locks for laptops and mobile devices.

   g. Recipient shall disable and/or immediately delete unused and terminated user accounts.

   h. Recipient shall implement annual intrusion penetration/vulnerability testing.

   i. Recipient shall encrypt Data at rest on central computing systems. Recipient shall also encrypt any backup, backup media, removable media, tape, or other copies. In addition, Recipient shall fully encrypt disks and storage for all laptops and mobile devices.

   j. Recipient shall provide annual, mandatory security awareness and Data handling training for all of its employees and/or students handling Data pursuant to this Agreement.

k. Recipient shall install and maintain on computers accessing or processing Data appropriate endpoint security anti-virus and anti-malware software. Recipient shall ensure all of Recipient's data processing systems, servers, laptops, PCs, and mobile devices are regularly scanned and have all security patches applied in a timely manner.

l. Recipient shall have physical security in buildings housing Data, along with controlled physical access to buildings and/or data centers.

m. Recipient's devices used to copy or scan hard copies of Data must have encrypted storage. Recipient shall scrub storage devices when equipment is retired. Hard copies containing Data are discouraged and must be physically secured, not left unattended, and physically Destroyed.

n. Box storage meets the encryption requirements within this MOU.

9. If Recipient becomes aware of an incident, misuse of Data, or unauthorized disclosure involving any Data, it shall notify Provider within one (1) calendar day and cooperate with Provider regarding recovery and remediation of the incident.

10. Provider may terminate this Agreement by provision of thirty (30) days prior written notice to Recipient.

11. Following the termination of this Agreement, Recipient shall, within thirty (30) calendar days, destroy all Data collected, generated, or inferred as a result of this Agreement.

12. Any notice required or permitted under this Agreement will be given in writing to an authorized representative of the other party, will reference this Agreement, and will be deemed effectively given either upon personal delivery to the party to be notified, three (3) business days after deposit with a reputable commercial overnight courier, with written verification of receipt, or on the date of facsimile transmission, provided that the notice is confirmed in another writing sent the following day by registered or certified mail. All notices will be sent to the addresses set forth below, or to such other address as may be specified by notice hereunder.

If to UT Tyler:
The University of Texas at Tyler
3900 University Blvd, Tyler, TX 75799
Attn: Richard C. Helfers, PhD
Email: rhelfers@uttyler.edu

If to Provider:
Flock Safety
1170 Howell Mill Rd NW Unit 210, Atlanta, Georgia
Attn: Andrea Korb
Email: andrea.korb@flocksafety.com
With a required copy to (in the case of legal notices):
Attn: Legal Department
Email: legal@flocksafety.com

13. This Agreement will be governed by the laws of the State of Texas.

14. This Agreement states the entire contract between the parties with respect to the subject matter of the agreement and supersedes any previous written or oral representations, statements, negotiations, or agreements. This Agreement may be modified only by written amendment executed by the authorized representatives of both parties.

15. Neither party may assign this Agreement without the prior written consent of the other party. The rights and obligations hereunder shall be binding upon and inure to the benefit of the parties' permitted successors and assigns.

16. Provider and Recipient are independent contractors and neither is an agent, joint venturer, or partner of the other.

17. Except as expressly provided above, nothing contained in this Agreement shall be deemed to grant to Recipient any right, title or interest in the Data.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed by their duly authorized representatives.

Flock Safety, Inc.

Name: Mark Smith

Title: General Counsel

Signature: DocuSigned by: Mark Smith AC5C921454C24F3... 11/1/2023

University of Texas at Tyler

Name: Kouider Mokhtari

Title: Interim Senior Vice President for Research

Signature: DocuSigned by: Kouider Mokhtari EF58D187AF54442...