EXHIBIT B

Data Collected by Kiosks

Data Collected by IKE Smart City Kiosks or Their Authorized Third-Party Vendors	**Data Not Collected, Stored, Disclosed, or Sold by IKE Smart City Kiosks or Their Authorized Third-Party Vendors**

Wi-Fi (if installed as determined by the City of Dallas and manually connected to by a user):
• Users must manually connect to the free Wi-Fi by selecting the IKE network and agreeing to the Terms of Service (no email required).
• To establish the connection, the system temporarily logs host names, IP addresses, **or** MAC IDs.
• These logs are automatically deleted within 30 days and are not used for any other purpose than to establish the Wi-Fi connection.
 	
Security Cameras (if installed as determined by the City of Dallas):
• Only 14 days of footage are stored locally on a DVR inside the kiosk and are automatically deleted after that period.
• Footage is available only to law enforcement upon formal request to IKE Smart City.
• Neither cities nor IKE staff have access to view or download footage independently.
• IKE's Operations Team will use the file transfer method preferred by the requesting law enforcement agency. If no preference is indicated, a secure, password-protected link will be shared using a trusted platform such as Dropbox or Microsoft OneDrive.
 	
Photobooth Feature (if a user of the kiosk opts to use this feature):
• Photos are stored for only 1 hour, long enough for users to retrieve them.
• Retrieval is done via a QR code that links to a private URL with a secure, unguessable key.
 	
SMS Capabilities (if enabled by the City of Dallas and if a user of the kiosk opts to use this feature):
	By default, IKE Smart City does not collect, store, disclose, or sell any user data. Our business model is focused solely on advertising displayed on kiosk screens—not on data monetization.
	
	Without user consent, IKE Smart City kiosks **do NOT** collect, store, disclose, or sell:
	• facial recognition
	• geolocation
	• evercookies
	• camera microphone access
	• gender profiling or eye tracking
	• age identification via AI models
	• license plate information
	• data to third-party vendors
	• MAC or IP addresses
	• any personally identifiable information (PII) from users or passersby such as:
	  ○ Usernames
	  ○ Addresses
	  ○ Gender
	  ○ Email addresses
	  ○ Phone numbers
	  ○ Date of birth
	  ○ Any other psychographic or demographic data

EXHIBIT B

• SMS features may be used to send photos or share kiosk directory information instead of scanning the QR code. • Message logs are stored by our provider (Twilio) and are deleted automatically once delivery is confirmed or after 1 hour—whichever comes first. *Pedestrian Counting (if enabled by the City of Dallas):* • The system collects anonymized MAC addresses. Newer phones send randomized MAC addresses by default; if a real MAC address is received, it is anonymized immediately by the manufacturer before IKE gains the ID. • Data used to determine whether a count is unique is immediately discarded. Only aggregated, non-identifiable statistics are retained. *Kiosk Usage Analytics:* • IKE Smart City anonymously tracks which applications are used and for how long. • A fully anonymized count of kiosk visits is maintained. • No individual user can be identified from this data. The analytics are used only to improve kiosk functionality and user experience.	

Cyber Security: We employ industry-leading security protocols including advanced firewalls, regular software updates, intrusion detection systems, and secure data encryption methods. Continuous monitoring for cybersecurity threats and vulnerabilities is conducted proactively to swiftly detect and mitigate potential security risks. This includes various automated security/vulnerability scans, regular updates and patching of our operating system, and yearly stress-testing by a third-party security firm. Finally, our entire system is a closed system with no way to plug in to the kiosk.

Additional Clarifications, Below:

- No user data is collected by default. We do not require anyone to sign up, log in, or otherwise provide information to use the kiosk.

EXHIBIT B

- Wi-Fi device counting is an optional feature we can provide but we use our own proprietary software developed in-house on top of our own hardware. There are no 3rd parties involved. Even though most devices now use anonymized/blank MAC addresses for network discovery, we take the added precaution of hashing and computing a fingerprint on-device prior aggregating and sending to our backend infrastructure.
- We do not store or collect device IDs or hostnames beyond what is needed for the Wi-Fi to operate if a user chooses to use the free WiFi. We own and operate all networking hardware not a 3rd party.
- Wi-Fi uses WPA3 encryption or better.
- At the time of the execution of this agreement, SMS/MMS functionality is disabled by default as of 2024 in favor of QR codes. It remains an option for some customers, but we are looking to phase it out.
- At the time of the execution of this agreement, all data uploads are encrypted using TLS 1.3, X25519, and AES 128 GCM.
- We do not store or collect mac addresses beyond what is required for the Wi-Fi to function at a fundamental level if someone chooses to use it.
- At the time of the execution of this agreement, data is stored in the cloud – AWS us-east-2 (Ohio).