EXHIBIT C

USE POLICY
Mobile Parking Payment Systems for Parking Management and Enforcement

Michael P. Ford
Parking & Mobility Division
Department of Transportation
City of Oakland

August 23, 2023

0. Definitions

Parking data
Any logbooks, records or data files used or created pursuant to a parking payment service including electronic storage media, Software, Source Code, any database and database rights, personal or personally identifiable information relating to an identified or identifiable individual, payment transaction, parking session or data transmission, including the originating and destination numbers and internet protocol address, date, time and duration, information on a vehicle, customer, location or payment media. This data may contain personally identifiable information (PII).

Personally identifiable information
Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

Raw Parking Payment Transaction Data
A subset of Parking Data that includes parking date, start and end times for each transaction, payment amounts, transaction fees for the Providers, numbered “zones” corresponding to parking location and customer data including license plate number, customer ID or other information about the customer and their payment media. This data may contain PII.

Unprocessed Anonymized Data
A subset of Raw Parking Payment Transaction Data that Includes parking transaction date with start and stop times for each transaction, meter payment amounts, user transaction fees for the Providers, and numbered “zones” corresponding to parking location. This data does not contain any PII or data on the customer except for the vehicle’s license plate number.

Aggregated Anonymized Data
A summary of Unprocessed Anonymized Data that Contains ONLY a sum of the total number of parking payment transactions that occurred on each block face during each one-hour period of each day and the total revenue received from the sum of those transactions. In any case where three or fewer transactions occurred on any given block face during any given hour, such data will be obfuscated to a default number. This will allow staff to know that a small number of

EXHIBIT C

transactions occurred, and revenue was collected, but also ensure that there is no record of any individual transactions. Therefore, this data does not contain any individual transaction data or customer data. This data does not contain any PII and cannot be used to re-identify anyone or their location.

Provider
A business whose services allow individuals to pay for parking sessions through a mobile phone application (app), website, or text message in Oakland and which has all necessary licenses and registrations to conduct such business.

Third Party Data Contractor
Any business contracted by the Provider to provide any service that may include accessing, storing or viewing Parking Data generated in Oakland.

System Security Plan
A plan submitted by each Provider detailing the data security, storage, and encryption practices that meet or exceed industry standards, including Payment Card Industry Data Security Standard (PCI-DSS) and System and Organization Controls 2 [e.g., (SOC 2). DOT expects that these best practices will primarily address user payment methods to protect credit card information. The Plan must also address how the Provider plans to prevent and respond to cyber-attacks, including:

- Process for keeping software up to date;
- Monitoring systems and networks for malicious activity;
- Use of secure uniform resource locators (URLs)
- Employee education and training;
- Who is responsible for reporting the attack to the appropriate authorities;
- How customers and others will be alerted;
- How Provider will discover what data and what kind of data was stolen;
- How the Provider will comply with CA Senate Bill 34; and
- Changing and strengthening passwords.

1. Purpose

The City of Oakland Department of Transportation (DOT) intends to enter into an agreement with five selected Providers whose services permit individuals to pay for parking sessions through a mobile phone application (app), website, or text message in Oakland. The five Providers are:

- PayByPhone US Inc. (PayByPhone),
- Passport, Inc. (Passport),
- ParkMobile, LLC (ParkMobile),
- HonkMobile USA Ltd. (Honk),
- IPS Group, Inc. (IPS).

EXHIBIT C

Agreements with each of these Providers will permit individuals in Oakland to pay for their parking sessions with Providers' services and in turn, share Parking Data and other relevant data connected with the service and Unprocessed Anonymized Data with DOT through online portals. All five Providers will comply with the City's Surveillance Technology Ordinance, including the approved use policy and impact report for this system, per the future revised agreement and scope of services (see **Appendix A**). Providers will process Raw Parking Payment Transaction Data collected in Oakland to show the following fields in the portal regarding parking sessions:

- Parker license plate (note: this data is necessary for DOT staff in the Parking Citation Assistance Center to respond to citation disputes)
- Transaction date
- Start and stop times
- User fee charged
- Parking (meter) fee charged
- Numerical zone corresponding to parking block

Per the requirements in the "City Data Addendum" to the standard professional services agreement (see **Attachment A**), Providers will maintain their respective online system portal/back-office systems with **none** of the following information visible to City staff at any time for any reason:

- Personally identifiable information (PII), including but not limited to, name, phone number, home address, email address, credit card information and user account details

Oakland is implementing "demand-responsive" parking areas in which parking fees may vary by block in order to reflect demand. So far, this has been limited to the Montclair business District and Chinatown but will be expanded to all of Oakland's business districts. In these areas, each block has a unique "zone" number. In these demand-responsive areas, zones will correspond to a City-provided Facility ID. This ID will be printed on new parking signs and will not differ by Provider. In all other metered parking areas prior to demand-responsive rates being implemented, the Provider-created ID per block will be used. When choosing to pay by app, customers must enter the zone number with the Provider's platform. Zones are shown in Providers' apps and on signs.

DOT is procuring a multi-provider mobile parking payment (pay by app) system in order to increase the convenience of this service to parkers, enhance data privacy and security components of the system, promote the use of this contactless payment method through a City-branded system, and more holistically support the active management of the parking system. A key improvement will be City of Oakland-branded signs in the public right of way (PROW) that will direct parkers to a webpage (oaklandca.gov/oakparkplus) with all available Providers, their transaction fees, and promotions. New City-branded signs will first be installed in Montclair and

EXHIBIT C

Chinatown before being installed in other metered areas. Parking meters are primarily located in commercial districts where demand for curbside spaces is highest.

By allowing multiple providers to operate in Oakland, visitors will likely not need to download any additional apps and share their information with another provider; rather, they are more likely to be able to use an existing app on their phone and conveniently pay for their parking session. They may also “shop around” among the five Providers to choose a Provider that best suits their needs based on promotions, transaction fees, registration requirements, and privacy policies. Providing more choices to parkers in Oakland may also minimize the number of Providers with whom users, especially visitors to Oakland, must share their information to access this payment option. Providers may compete for long-term customers with lower user fees and promotions, and from new community engagement requirements intended to make Providers’ services more equitable and inclusive.

DOT receives Unprocessed Anonymized Data to reconcile parking payments, to enforce parking restrictions, such as time limits and meter payments, and to review citation disputes. License plate information is particularly critical to staff issuing citations and processing disputed citations. In receiving Unprocessed Anonymized Data, DOT can confirm that parking rates are accurately charged to parkers, that the City receives accurate parking payments, particularly from parkers in demand-responsive parking program areas, and that citations were issued correctly, in the event that a parking citation is contested over an active mobile payment session. For example, in demand-responsive areas, meter rates change by time of day and block; if staff could not see the zones in transaction data, DOT would not be able to program these specific areas’ rates or confirm the accuracy of Providers’ rates or revenues in reconciliations and audits. Outside the portal, DOT staff’s parking data analyses may summarize this data by zone, date, hour, transaction type, parking duration, or amount. When summarizing by zone (location), staff will use Census blocks for spatial analyses.

The City receives Aggregated Anonymized Data (which does not include license plates) from Providers in order to analyze parking revenues and demand. These uses ultimately inform parking policies and practices that support the City’s Parking Principles (Resolution No. 84664 CMS) and shape a more equitable mobility system. Notably, parkers are not and will not be required to use the mobile parking payment system in on- or off-street facilities in Oakland, as the California Vehicle Code requires a physical payment option.[1] As noted above, user account details containing PII will not be visible to City staff in each of the Providers’ portals. This data is not necessary to City staff’s management or enforcement of the parking system and thus, will not be displayed in the portal.

2. Authorized Use

[1] California Vehicle Code Section 22508.5(d) is available online here: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=VEH&sectionNum=22508.5

EXHIBIT C

Only designated DOT and Finance Department staff will have access to the most recent year of Unprocessed Anonymized Data received from Providers through unique portal credentials. Specific applications of mobile parking payment data that supports this effort will include only the following:

a) Reconciling payment transactions with total parking revenues received
b) Promoting compliance and enforcing parking restrictions, permits, and payment
c) Reviewing contested parking citations
d) Remitting user transaction fees to Providers via invoices

Designated DOT and Finance Department staff will also have access to Aggregated Anonymized Data received from Providers through unique portal credentials. Use of this data (which exclude PII and are unable to be re-identified) may include, but is not limited to, the following:

e) Estimating parking demand, occupancy, and revenues by block face
f) Evaluating parking payment options
g) Monitoring demand-responsive parking areas and general levels of compliance with parking rules

DOT staff may use Aggregated Anonymized Data in public reports, post it to the City's open data portal or otherwise make it available for public use.

3. Data Collection

Mobile parking payment users generate Parking Data by making transactions for parking. Providers collect Raw Parking Payment Transaction Data from these transactions and push Unprocessed Anonymized Data and Aggregated Anonymized Data to their portal for DOT and Finance staff to view. As stated in Section 1, Unprocessed Anonymized Data will never include PII. Rather, this dataset will include parking date and start and end times for each transaction, payment amounts, transaction fees for the Providers, and numbered "zones" corresponding to parking location.

The Providers must collect Raw Parking Payment Transaction Data in order to process financial transactions in compliance with their System Security Plan, including Payment Card Industry Data Security Standard (PCI-DSS), System and Organization Controls 2 (SOC 2), and Senate Bill No. 34. All five selected Providers currently maintain PCI-DSS and SOC 2 compliance and must continue to do so.

4. Data Access

Only authorized staff from the DOT and the City's Finance Department will have access to the most recent year of Unprocessed Anonymized Data. Data will be accessed through Providers' online platforms. Authorized users of the online platforms will require a unique username and

EXHIBIT C

password. Because all data in the platform will have no personally identifiable information or individual user account information, any data shared outside the platform, such as through public records requests, court orders, or in the City's Open Data Portal, will be anonymous, thus prohibiting City staff from identifying individuals from this parking data. Anyone can have access to the Aggregated Anonymized Data. Staff may upload Aggregated Anonymized Data to the City's open data portal for easier public access.

5. Data Protection

DOT will depend on each Provider to securely store, transmit, and audit transaction and user data per requirements in their Scope of Services and per industry best practices. Providers will also be required to provide a System Security Plan with data security, storage, and encryption practices that meet or exceed industry standards, including Payment Card Industry Data Security Standard (PCI-DSS) and System and Organization Controls 2 [e.g., (SOC 2). All five Providers comply with PCI-DSS and SOC 2 standards at a level corresponding to their number of annual transactions processed. DOT expects that these best practices will primarily address user payment methods to protect credit card information.

All five Providers also have existing user terms and conditions and privacy policies available for their services (see **Appendix B** and **Appendix C**).

However, all Providers will be required to accept and comply with the "City Data Addendum" to the professional services agreement (see Attachment A), including the approved use policy and impact report for this system, upon the signing of their respective agreements. DOT also requires that every Provider has a secure gateway service for secure (encrypted) credit card data transmission to the City's merchant account Provider.

DOT staff worked with the Capital Contracts Division and the City Attorney's Office to include the requirement to comply with the approved Use Policy and Impact Report for this system in the Provider's Professional Services Agreement. By situating this requirement in the body of that agreement, in addition to the scope of services (see **Appendix A**), the City will have greater capability to enforce this requirement in the event of non-compliance. The existing agreement language, as edited by the City Attorney's Office, can be found in **Appendix D**.

6. Data Retention

Under the existing agreement with ParkMobile, the precedent for retaining mobile parking payment data in their portal is two (2) years. However, staff will reduce this requirement to one (1) year. At least one year is needed in order to provide sufficient time for parking citation appeal processes.

Raw Parking Payment Transaction Data is unaggregated, unsummarized data for each parking event. Providers will store all Raw Parking Payment Transaction Data collected in Oakland for no more than one (1) year. If the contract between a Provider and DOT is severed, the Provider will be required, per the signed Professional Services Agreement, to delete all Raw Parking Payment Transaction Data collected in Oakland (see **Appendix A**). If such contract severance occurs, the Provider will email the DOT Project Manager, within 30 days of contract severance, a confirmation that all raw data collected in Oakland has been deleted.

Unprocessed Anonymized Data Includes parking transaction date with start and stop times for each transaction, meter payment amounts, user transaction fees charged by the Providers, and numbered “zones” corresponding to parking location. Unprocessed Anonymized Data does not contain any data on the customer except for the vehicle’s license plate number. This data will be stored by Providers and the City for no more than one (1) year.

Aggregated Anonymized Data is a processed version of Unprocessed Anonymized Data that does not include any data on individual transactions. It contains only a sum of the total number of transactions that occurred on each block face during each one-hour period of each day and the total revenue received from the sum of those transactions. This data is important for staff to examine long-term trends in parking occupancy and revenue. If the contract between a Provider and DOT is severed, the Provider will be required per the signed agreement to delete all Aggregated Anonymized Data generated in Oakland. The City may retain this data indefinitely.

Staff currently do not have access to any ParkMobile user account information and will continue to not have this access to protect user privacy. With multiple providers now competing for Oakland parkers’ payments, staff will not ask ParkMobile to migrate user information or data to any of the new Providers operating under the upcoming mobile parking payment system. Parkers may continue to use ParkMobile in Oakland, or any other selected Provider’s app of their choosing.

7. Public Access

The public may access the Aggregated Anonymized Data provided in each Provider’s portal through public records requests. Aggregated Anonymized Data may also be added to the City’s Open Data Portal. Raw Parking Payment Transaction Data and Unprocessed Anonymized Data will only be released as required by law under subpoenas, warrants, or other court orders.

8. Third-Party Data-Sharing

Providers collect and generate Parking Data associated with the mobile parking payment system. Providing only Unprocessed Anonymized Data and Aggregated Anonymized Data in the portal that Providers give to City staff (removing PII) reduces the risk of surveillance and eliminates the possibility of user identification by City staff. However, staff understand that a primary concern is the security of the Third Party Data Contractors that Providers use, particularly following the ParkMobile data breach in March 2021.

Providers may contract with Third Party Data Contractors to process and/or store data. If using Third Party Data Contractors, Providers must:

- Mandate to any Third Party Data Contractors that they follow the same System Security Plan terms as the Providers; and
- Only provide access to Unprocessed Anonymized Data and/or Aggregated Anonymized Data; and
- Disclose to users, in the Providers' privacy policies, what data is shared with third parties (see **Appendix B**).

Providers may not share or sell Parking Data collected in Oakland with any third parties except for:

- Third Party Data Contractors that are contracted with for legitimate and necessary data services such as data storage and processing and subject to the terms listed above; and
- Aggregated Anonymized Data.

Notably, DOT does not have the capacity or means to create a mobile parking payment service in-house specific to Oakland parkers and is thus reliant on the selected Providers' services. Because working with third parties to securely store data is a widespread industry practice, staff believe that Providers are in a similar position – they do not have the capacity or means to securely process and/or store millions of parking transaction data in-house.

9. Training

Each Provider is required to provide web-based or on-site training for authorized City staff in the DOT Parking & Mobility Division, the Finance Department, or both (see **Appendix A**).

10. Audit and Oversight

As shown in the draft Professional Services Agreement scope (see **Appendix A**), all five selected Providers are required to provide a fully auditable mobile parking payment service. DOT or Finance staff will audit Providers through their respective back-end online data portals, in addition to Providers going through PCI DSS audits and any other audits that Providers have independently arranged. Audits by DOT or Finance staff will occur on an as-needed basis, such as audits of a sub-set of zones where meter rates were recently changed. General oversight of the Providers are the responsibility of the Parking & Mobility Division Manager. The legally enforceable sanctions for violations of the policy include relevant administrative instructions as well as provisions in the Surveillance and Community Safety Ordinance.

11. Maintenance

Providers are responsible for maintaining and managing all data generated through their respective app, website, and text message services. As noted in the Third-Party Data-Sharing section of this report, Third Party Data Contractors are generally used by Providers for storage and/or security purposes.

EXHIBIT C

Questions or comments concerning this draft Use Policy should be directed to Michael Ford, Division Manager, Parking and Mobility Division, via email at mford@oaklandca.gov or phone at (510) 238-7670.