CITY OF OAKLAND

Privacy Advisory Commission

July 6, 2023 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
Regular Meeting Agenda

***Commission Members**: **District 1 Representative**: Reem Suleiman, **District 2 Representative**: Chloe Brown, **District 3 Representative**: Brian Hofer, Chair, **District 4 Representative**: Lou Katz, **District 5 Representative**: Omar De La Cruz, **District 6 Representative**: Gina Tomlinson, **District 7 Representative**: Robert Oliver, **Council At-Large Representative**: Henry Gage III, Vice Chair, **Mayoral Representative**: Jessica Leavitt*

Each person wishing to speak on items must fill out a speaker's card. Persons addressing the Privacy Advisory Commission shall state their names and the organization they are representing, if any.

1. Call to Order, determination of quorum

2. Open Forum/Public Comment

3. Surveillance Technology Ordinance – DOT – Mobile Parking Payment System
    a. Review and take possible action on the proposed use policy

4. Surveillance Technology Ordinance – OPD – Annual Reports
    a. Review and take possible action on the annual reports for ShotSpotter, Forensic Logic/Coplink, Automated License Plate Readers (ALPR)

5. Surveillance Technology Ordinance – OPD – Fixed Wing Aircraft (with surveillance technology)
    a. Review and take possible action on a proposed use policy

6. Surveillance Technology Ordinance – OPD – Automated License Plate Readers (ALPR)
    a. Review and take possible action on a proposed use policy

Each person wishing to speak on items must fill out a speaker's card. Persons addressing the Privacy Advisory Commission shall state their names and the organization they are representing, if any.

Members of the public can view the meeting live on KTOP or on the City's website at https://www.oaklandca.gov/topics/ktop-tv-10.

Comment in advance. To send your comment directly to the Privacy Commission and staff BEFORE the meeting starts, please send your comment, along with your full name and agenda item number you are commenting on, to Felicia Verdin at fverdin@oaklandca.gov. Please note that eComment submissions close one (1) hour before posted meeting time. All submitted public comment will be provided to the Privacy Commission prior to the meeting.

Each person wishing to speak on items must fill out and submit a speaker's card to staff prior to the meeting. Members of the public can address the Privacy Advisory Commission in-person only and shall state their names and the organization they are representing, if any.

To observe the meeting via Zoom, go to: https://us02web.zoom.us/j/85817209915
Or One tap mobile: +1 669 900 9128

USE POLICY - REVISED DRAFT
Mobile Parking Payment Systems for
Parking Management and Enforcement

Michael P. Ford
Parking & Mobility Division
Department of Transportation
City of Oakland
April 28, 2023

1. Purpose

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

- PayByPhone US Inc. (PayByPhone),
- Passport, Inc. (Passport),
- ParkMobile, LLC (ParkMobile),
- HonkMobile USA Ltd. (Honk),
- Marina Security Services, Inc. and Mortimer Smythe LLC (Oakland Parking Solutions), and
- IPS Group, Inc. (IPS).

Agreements with each of these Providers will permit individuals in Oakland to pay for their parking sessions with Providers' services and in turn, share data on parking transactions with DOT through online portals. All six 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 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), such as phone number and email address
- Individual user account details, such as email address, phone number, and credit card information

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, but will be expanded to Chinatown and then all of Downtown. 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-vendor 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 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 vendors to operate in Oakland, visitors will likely not need to download any additional apps and share their information with another vendor; 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 six 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. Vendors 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 parking data from Providers in order to analyze parking revenues and demand, 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. 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, individual user account details (such as email, phone number, credit card information) and 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.

In receiving parking 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.

2. Authorized Use

Only designated DOT and Finance Department staff will have access to the anonymized data (excluding PII and user account details) received from Providers through unique portal credentials. Specific applications of mobile parking payment data that supports this effort will include only the following:

a) Estimating parking demand, occupancy, and revenues
b) Evaluating parking payment options
c) Monitoring demand-responsive parking areas and compliance
d) Reconciling payment transactions with total parking revenues received
e) Promoting compliance and enforcing parking restrictions, permits, and payment
f) Reviewing contested parking citations
g) Remitting user transaction fees to Providers via invoices

Parking policies and practices informed by this data are intended to support the City's Parking Principles (Resolution No. 84664 CMS) and shape a more equitable mobility system. For example, DOT staff have analyzed parking payments made by credit/debit card, coin, and ParkMobile to better understand the expenses in the parking system, such as those paid to the City's merchant bank and to the City's meter vendor. As parking revenues have historically made up a significant portion of the General Fund, this analysis helped staff understand how to minimize expenses where possible.

3. Data Collection

[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

DOT will receive anonymized parking data through the selected Providers' platforms. Mobile parking payment users generate data by making transactions. Providers collect raw data from these transactions and push processed data to their portal for DOT and Finance staff to view. As stated in Section 1, this dataset will never include PII or individual user account details. Rather, this dataset will include parking date and start and end times, payment amounts, transaction fees for the Providers, and numbered "zones" corresponding to parking location. The Providers collect this data in order to process financial transactions in compliance with Payment Card Industry Data Security Standard (PCI-DSS). All six selected Providers currently maintain PCI-DSS compliance and will continue to do so.

4. Data Access

Authorized staff will only be from the DOT and the City's Finance Department. Data will be accessed through Providers' online platforms. Authorized users of the online platforms will require a unique username and 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.

5. Data Protection

DOT will depend on each Provider to securely store, transmit, and audit transaction and user data per language in the Scope of Services and per industry best practices. All six Providers comply with PCI-DSS standards at a level corresponding to their number of annual transactions processed. Five of six Providers also have existing user terms and conditions and privacy policies available for their services (see **Appendix B** and **Appendix C**). Only Oakland Parking Solutions, a local company that is custom-building an app for Oakland, does not have these documents available for review yet.

However, all Providers, including Oakland Parking Solutions, 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 are currently working with the Capital Contracts Division and the City Attorneys Office to include the requirement to comply with the approved use policy and impact report for this system in the Professional Services Agreement. By situating this requirement in the body of the 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 to be edited by the City Attorneys 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 in order to provide sufficient time for parking citation appeal processes. In addition to this processed, anonymous data shown in their portals, Providers will store raw (unaggregated) 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 agreement to delete all raw parking payment transaction data collected in Oakland (see **Appendix A**). If such an event occurs, the Provider will email the DOT Project Manager a confirmation that all raw data collected in Oakland has been deleted.

Staff currently do not have access to any user account information and will continue to not have this access to protect user privacy. With multiple vendors 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 anonymized data provided in each Provider's portal through public records requests, subpoenas, warrants, and other court orders. Anonymized mobile parking payment data may also be added to the City's Open Data Portal.

8. Third-Party Data-Sharing

Providers collect and generate the raw data associated with the mobile parking payment system. Anonymizing this data in the portal that Providers give to City staff (removing PII and user account details) 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 services that Providers use, particularly following the ParkMobile data breach in March 2021. Providers may use third party services to process or store data. Providers' privacy policies disclose to users what data is shared with third parties (see **Appendix B**).

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 agreement scope (see **Appendix A**), all six 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 parties are generally used by Providers for storage and/or security purposes.

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.

ANTICIPATED IMPACT REPORT - REVISED DRAFT
Mobile Parking Payment Systems for
Parking Management and Enforcement

Michael P. Ford
Parking & Mobility Division
Department of Transportation
City of Oakland
April 28, 2023

1. Information Describing the Proposed Data Sharing Agreement and How It Works

The City of Oakland (City) Department of Transportation (DOT) intends to enter into agreements with each of the six selected providers (Providers), including:

- PayByPhone US Inc. (PayByPhone),
- Passport, Inc. (Passport),
- ParkMobile, LLC (ParkMobile),
- HonkMobile USA Ltd. (Honk),
- Marina Security Services, Inc. and Mortimer Smythe LLC (Oakland Parking Solutions), and
- IPS Group, Inc. (IPS).

These Providers' services permit individuals to pay for parking sessions through their mobile phones in Oakland. With these services, parkers will be able to initiate a parking session through a mobile phone application (app), website, text message, or phone call, depending on the Providers' services. To initiate a parking session, parkers are required to enter their payment information (such as a credit card or Google Pay), "zones" corresponding to City blocks, and license plate number on the Providers' app. Oakland is implementing "demand-responsive" parking areas in which parking fees may vary from block to block in order to reflect demand. So far, this has been limited to the Montclair business District, but will be expanded to Chinatown and then all of Downtown. In these areas, each block has a unique "zone" number. In demand-responsive areas, zones will correspond to a City-provided Facility ID 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 uses parking data from mobile parking payment Providers in order to enforce parking restrictions, such as time limits and meter payments, to analyze parking revenues and demand, and to review citation disputes. License plate and zone information are pushed to DOT's

Automated License Plate Readers (ALPR)[1] through an application programming interface (API) between other vendors who support the City's parking enforcement system. Parking Control Technicians use ALPR to scan vehicles' license plates and check for an active ParkMobile session associated with the license plate and location (numbered zone).

In addition to pushing data to enforcement technologies, the Providers also collect data from parking sessions and "publishes" these datasets to an online platform that authorized staff can access through a unique username and password. The data published to the online platform will be provided from parkers' transactions and include license plate number, parking date and start and stop times, payment amounts, transaction fees for the Providers, and "zones" corresponding to parking location. This data will include no personally identifiable information, and DOT staff will use this data for financial and parking analyses and for responding to parking citation disputes. Outside the portal, DOT staff will analyze and summarize this data by zone, date, hour, transaction type, device type, parking duration, or amount. When summarizing by zone (location), staff will use Census blocks for spatial analyses.

In receiving parking data, DOT can ensure that programmed parking rates and time limits are accurate and parking citations are correctly issued. For example, in an event a parker disputes a citation due to having a paid ParkMobile session, the parking payment can be properly reconciled, particularly in demand-responsive parking program areas.[2] In these areas, meter rates change by time of day and Value or Premium Rate area. DOT will ensure that zones would be visible in the transaction data in order to program these specific areas' rates or audit the accuracy of Providers' rates/revenues. The importance of this auditability recently came up regarding the demand-responsive rates at the La Salle Garage and in Montclair, where time-of-day pricing was not correctly programmed in ParkMobile's app and showed this incorrect pricing to parkers. This error had financial implications but was able to be corrected through the portal and through ParkMobile's client support services.

The professional service agreements with each Provider will allow Providers to share parking data, including location-based information corresponding to numbered block zones, with DOT. Importantly, the agreements will require that certain data is excluded from the portal in order to better protect individual parkers' privacy (see excerpt below). DOT staff will be able to access up to one (1) year of processed, anonymous parking data in each Provider's online portal. If a contract between a Provider and the City is severed, then the Provider will be required to delete all raw parking data collected in Oakland. City staff will not have access to raw parking data in this portal. For additional details, see the draft "City Data Addendum" to the City's Professional Services agreement (Attachment A).

[1] See the Privacy Advisory Commission's approved use policy and anticipated impact report for automated license plate readers. Available online at: https://www.oaklandca.gov/documents/automated-license-plate-reader

[2] More information on ParkOakland, the Demand-Responsive Parking & Mobility Management Initiative, is available on the City's website here: https://www.oaklandca.gov/topics/park-oakland

The contract term is for up to seven years, including two optional years, and in an annual amount not to exceed $900,000 in Providers' transaction fees collected from parkers in Oakland.

DOT staff have aimed to procure the most secure mobile parking payment system through the RFP process. The Request For Proposals (RFP) was issued in March 2022, and proposals were due in April 2022. DOT staff received seven proposals, of which six were deemed Responsive. When DOT staff initially presented the next-generation mobile parking payment system to the PAC in April 2021, data security for users was a key component of discussion. The Commission's comments were adopted into the RFP, primarily through the following scope section:

> ***1.4 Data Privacy Requirements.*** *One of the key goals of this new pay-by-phone system is to enhance user data protections. The system must comply with the City's Surveillance Technology Ordinance (Oakland Municipal Code Chapter 9.64) and subsequent system use policy and anticipated impact report in the following capacities:*
>
> - *Maintain an online system portal/back-office system with **none** of the following information visible to staff at any time for any reason:*
>   - *Personally identifiable information (PII), such as phone number and email address*
>   - ~~*Customer license plate information (note: this information must be visible for real-time enforcement purposes, but not to office staff accessing the online portal)*~~[3]
>   - *Individual user account details*
> - *Provide a system with data security, storage, and encryption practices that meet or exceed industry standards. DOT expects that these best practices will primarily address user payment methods to protect credit card information.*
> - *Disclose any additional companies who would support the Consultant's system, such as third-party cloud storage services.*
> - *Ensure the security of user and transaction data through security protocols per current industry standards.*
> - *Provide a data storage and privacy system that meets or exceeds industry standards. Consultant must comply with the City's Surveillance and Community Safety Ordinance (Oakland Municipal Code Chapter 9.64), the approved use policy regarding the mobile parking payment system, and any other relevant surveillance laws relevant to Oakland, California.*

[3] Though this was a requirement provided in the RFP, new information has arisen that this license plate data is necessary for DOT staff to respond to parking citation disputes. Per the current Parking Citation Assistance Center's standard operating procedures, parker license plate, zone number, and parking session start date and time are essential data to staff's determination if a citation was issued correctly. Thus, staff are planning to remove this section from the scope of services.

Notably, parkers are not required to use the mobile parking payment system in on- or off-street facilities in Oakland. The California Vehicle Code requires that parking meters must be operable in order to write a defensible citation; in other words, parking payment for a space cannot only be accepted by nonphysical means like an app or website (CVC Section 22508.5(d)).[4] While there is no anticipated possibility that parkers will be required to use the new mobile parking payment system in Oakland, DOT staff seek to implement a system that meets, if not exceeds, the requirements of the Surveillance Technology Ordinance.

DOT staff worked with Contract Services and the City Attorneys Office to include the requirement to comply with the approved use policy and impact report for this system in the Professional Services Agreement. By including this requirement as an addendum of the standard professional services agreement (see Attachment A), the City will have greater capability to enforce this requirement in the event of non-compliance. The existing agreement language to be edited by the City Attorneys can be found in **Appendix D**.

2. Proposed Purpose

Data from mobile parking payment services currently shape parking policies, plans, and practices in Oakland. Analyses of this data guide staff's active management of the parking system and access to finite, valuable curb space. Importantly, this data is also used in the issuance of citations and the review of citation disputes. Mobile parking payment services expand the available payment options for parkers, in turn increasing the convenience and ease of parking. Making parking easy and more actively managing the parking system are two of the City's Parking Principles (Resolution No. 84664 CMS) and shape a more equitable mobility system.

Under the current mobile parking payment system, a single Provider is permitted to operate in Oakland. From 2015 to 2019, parking payments made through this Provider comprised about 10% to 15% of the City's total on-street parking revenue, generating a total of approximately $6.5 million in parking revenues. Signage promoting this Provider's brand is currently posted in the public right-of-way (PROW) but given maintenance challenges, is not always readable. The City's current Provider, ParkMobile, also supports ongoing pilots at the LaSalle Garage in the Montclair District and the Telegraph Plaza Garage to integrate the City's off-street facilities into the on-street system and thus, eliminate costly one-time expenses such as traditional parking access and revenue control systems (PARCS), and ongoing expenses, such as administrative and accounting overhead, maintenance of equipment, and back-office labor. This integration was adopted by City Council in the Fiscal Year 2021-2022 Budget.

DOT has pursued an enhanced multi-vendor mobile parking payment system for several reasons: 1) increase the convenience of this service to parkers, 2) promote the use of this contactless payment method with City-branded signs in the PROW, and 3) more holistically support the active management of the parking system. A key improvement will be City of

[4] This CVC section is available online here: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=VEH&sectionNum=22508.5

Oakland-branded signs that will direct parkers to a webpage with all available Providers and promotions, as well as supporting future pilots and innovations like the LaSalle Garage. Existing ParkMobile signs that display the zone number are currently in a state of severe disrepair, when they are still present on-street at all (see **Figure 1**). New City-branded signs will be printed and installed in demand-responsive project areas in phases, as meter rates are adjusted and Value and Premium Rate areas implemented (see **Figure 2**). Signs in Montclair and bilingual signs in Chinatown will be implemented first. Providers will contribute to the costs of installing and maintaining the system, particularly signs, through a one-time up-front fee of $190,000 (split across all selected Providers) and 10% of ongoing user fees. In addition to these fees, Providers may run their own marketing campaigns aimed at parkers in Oakland.

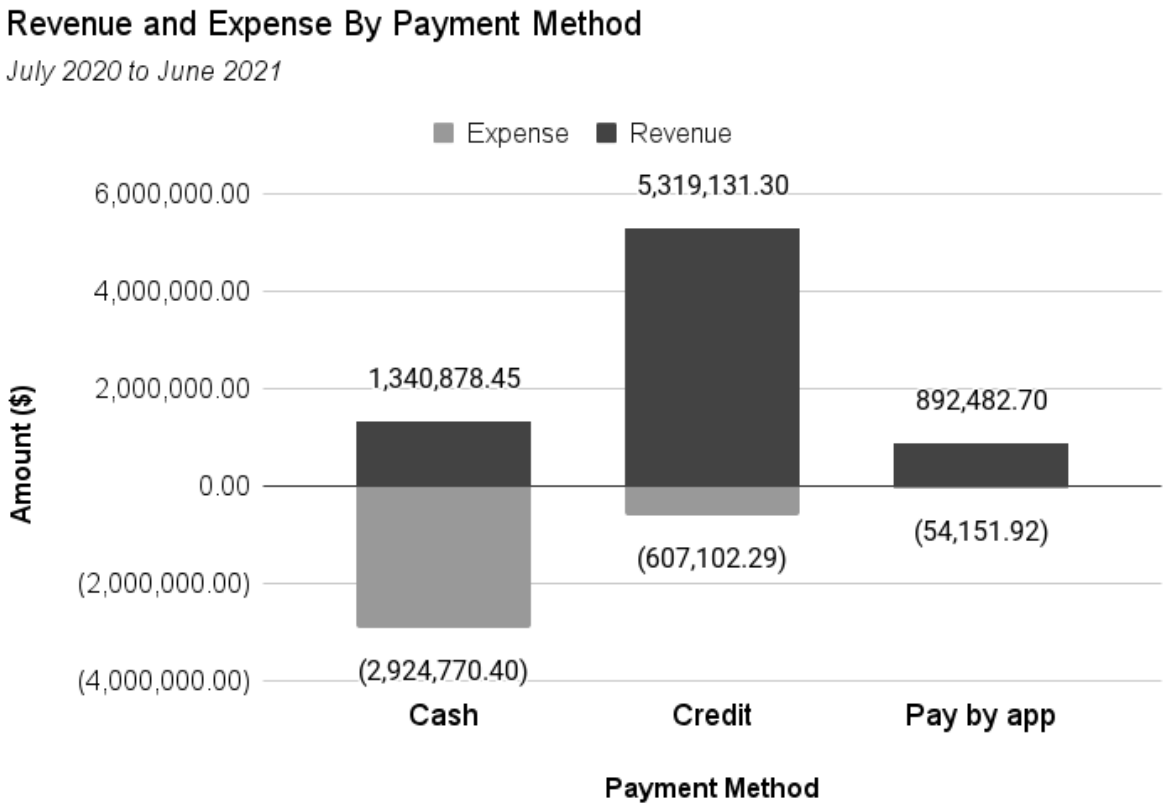
Figure 1: Existing Pay Here + Mobile Parking Payment Signs

Figure 2: New Approved Pay Here + Mobile Parking Payment Signs

The mobile parking payment system provides several key advantages to both parkers and the City that contribute to the importance of this system. The mobile parking payment system meets rising demand for contactless payment options and supports the health and safety of consumers by reducing touch-points.[5] It is anticipated that positive consumer experiences with contactless payments, including the City's pay-by-app parking services, will make more individuals interested in using this payment type, even as the pandemic continues to subside. Additionally, the City pays lower fees for parking transactions made by app than transactions made by coin or credit/debit card (see **Figure 3**). In Fiscal Year 2020-2021, 6% of parking revenues paid by app were spent on fees and expenses, compared to 11% spent on credit/debit card expenses and 218% on coin expenses.

Figure 3: Revenue and Expense by Payment Method (July 2020 to June 2021)

[5] Retail Leader. "Will Consumers Stick With Contactless Payments?" August 6, 2020. Available online here: https://retailleader.com/will-consumers-stick-contactless-payments



By accepting multiple vendors to operate in Oakland, visitors will likely not need to download any additional applications (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. With this variety of Provider options available to parkers, the enhanced system is intended to minimize the number of Providers with whom users, especially visitors to Oakland, must share their information to pay for parking by app and maximize parkers' choices as consumers.

Residents will also benefit from having multiple vendor options, as vendors will compete for long-term customers with lower user fees and promotions, and from new community engagement requirements that aim to make Providers' services more equitable and inclusive. Each Provider's user fee and website will be clearly shown on the City's go-to parking resource webpage (oaklandca.gov/oakparkplus). A QR code and the URL to this webpage are shown on the new City-branded signs to be installed in demand-responsive project areas.

Specific applications of mobile parking payment data that supports this effort will include only the following:

a) Estimating parking demand, occupancy, and revenues
b) Evaluating parking payment options

c) Monitoring demand-responsive parking areas and compliance
d) Reconciling payment transactions with total parking revenues received
e) Promoting compliance and enforcing parking restrictions, permits, and payment
f) Reviewing contested parking citations
g) Remitting user transaction fees to Providers via invoices

3. Locations of Deployment

The data shared under this proposed agreement is user-generated within the City's parking system and therefore collected in all neighborhoods with parking meters or public parking facilities. Parking meters and public parking facilities are primarily found in commercial zones, near public transit stations, and in other areas with high demand for parking. Existing meters and Council-approved meter zones (OMC Section 10.36.140) are shown in this map: https://oakgis.maps.arcgis.com/apps/mapviewer/index.html?webmap=8fa241d70ab5494f8e50e678065d627b

While new signs showing new zone numbers will be installed first in Montclair and Chinatown, the Providers will operate in all metered areas. Providers may begin operating in phases, such as if beta testing is required, and may start in certain geographic areas before operating at citywide scale. In this case, the geographic areas where Providers operate would be listed on the City's parking webpage to minimize any confusion to parkers and appropriately communicate how to use the mobile parking payment system.

4. Potential Impact on Civil Liberties & Privacy

DOT acknowledges the private and sensitive nature of personally identifiable information (PII) and block-level location data included in mobile parking payment data. Without mitigations, mobile parking payment data would be vulnerable to privacy risks such as re-identification, as users' names and contact information are typically collected by Providers and made available to their clients via the portal. In order to minimize, if not eliminate, privacy and surveillance risk, DOT has developed a set of guidelines based on feedback from the Privacy Advisory Commission received in March and April 2021 for how mobile parking payment data will be handled and obfuscated to protect users' data, using mitigations outlined below. These mitigations were provided to prospective bidders in the recent competitive process for the enhanced mobile parking payment system; through their proposals, all six Providers have initially agreed to follow the mitigations below and this impact report and use policy, upon finalization and approval.

In addition to the City's requirements to enhance privacy, five of the six Providers have privacy policies that apply to their platform specifically (see **Appendix B**). Under this new mobile parking payment system, parkers will have five more options for paying for parking than they currently do. Each privacy policy is available for an individual's review online and through the Providers' apps, so privacy can be a factor by which parkers make a decision.

5. Mitigations

DOT recognizes the sensitive nature of parking and user data generated through mobile parking payment Providers and has developed the following guidelines for the responsible handling of this data:

1. Per the draft agreement scope (see **Appendix A**), DOT will not have access to any PII of parkers who use the Providers' services. The public may access anonymized minimally-processed data available in the portal through public records requests, subpoenas, warrants, and other court orders. This data will not be raw, as Providers will have removed PII and individual user account details from the portal.
    a. In the competitive process to procure the new mobile parking payment system, DOT issued the requirement below. All six proposed Providers have initially agreed to this requirement in their respective proposals. This mitigation would effectively eliminate privacy risk by anonymizing parking data.

    - *"Maintain an online system portal/back-office system with **none** of the following information visible to staff at any time for any reason:*
        - *Personally identifiable information (PII), such as phone number and email address*
        - ~~*Customer license plate information (note: this information must be visible for real-time enforcement purposes, but not to office staff accessing the online portal)*~~[6]
        - *Individual user account details"*

2. DOT has sought and selected Providers whose data security, storage, and encryption practices meet or exceed industry standards. All Providers currently and must continue to maintain Payment Card Industry Data Security Standard (PCI-DSS) compliance. Additional privacy and security measures, such as California Consumer Protection Act compliance, differs between Providers but is available in their respective privacy policies (see **Appendix B**).
3. After each agreement has been signed and executed, login credentials to the Providers' online portals will be unique to each authorized staff who has been granted access to the mobile parking payment data. Login credentials will not be shared outside of authorized staff in DOT and Finance.

6. Data Types and Sources

[6] Though this was a requirement provided in the RFP, new information has arisen that this license plate data is necessary to respond for DOT staff to parking citation disputes. Per the current Parking Citation Assistance Center's standard operating procedures, parker license plate, zone number, and parking session start date and time are essential data to staff's determination if a citation was issued correctly. Thus, staff are planning to remove this section from the scope of services.

In this proposed system, the Providers will “publish” parking data on their respective online platforms. While these platforms vary by Provider, parking data available within the platform will include the following:

- Numbered zone indicating approximate parking location
- Parking date and start and end times
- Parking transaction amount
- Transaction fee (to be paid to the Provider)

Provider’s portals primarily differ by aggregate data analyses, such as charts and graphs showing growth over time in Oakland parking transactions made by app. Importantly, as stated in the previous section no Provider will show PII or individual user accounts in the portal at any time for any reason.

Regarding license plate numbers, this data is necessary for both enforcement purposes and for responding to parkers’ citation disputes. License plates are scanned or entered by Parking Control Technicians in automated license plate readers (ALPR) to check if the vehicle has an active parking session. All citations issued require that a license plate number be inputted, and the handheld device prohibits a Parking Control Technician from issuing and printing the citation if there is an active ParkMobile session associated with the plate. In the event that a parking citation is disputed, then this request is processed and analyzed by the Parking Citation Assistance Center Staff. Currently, staff look up the license plate number in ParkMobile’s portal and verify their parking session by license plate, zone number, and parking session date and start time. Without being able to view license plate information, Parking Citation Assistance Center staff would have to rely on vendors to look up this data, which would pose a significant burden on the Center’s processing time and resources.

Only authorized staff in DOT and the Finance Department with unique usernames and passwords may log in and access this data, unless requested through a public records request.

7. Data Security

Each provider responded with details regarding their own unique data security protocols. Per the draft agreement section in Section 1 of this impact report, DOT is requiring that each Provider securely store, publish, and audit the data according to industry standards and best practices. 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. Audits by DOT or Finance staff will occur on an as-needed basis, such as audits of a subset of zones where meter rates were recently changed.

Upon execution of the draft agreements (see **Appendix A**), Providers are required to provide a current certification through the Payment Card Industry Data Security Standards (PCI DSS). All Providers currently meet these standards. Major Providers such as ParkMobile, Passport, and

PayByPhone maintain PCI DSS Level 1 certification. Smaller Providers may maintain a lower level due to the smaller number of annual transactions processed through them. PCI DSS certification was the primary security requirement that the City sought when procuring mobile parking payment services in 2015 and continues to be industry standard. Procurement of the new mobile parking payment system has sought to maintain and exceed this standard through additional privacy and security requirements by disclosing data storage and encryption practices and PII protection.

Auditability was also a requirement of the 2016 agreement between the City of Oakland and ParkMobile, and ParkMobile has published information regarding account and payment security on its website: https://support.parkmobile.io/hc/en-us/articles/203299650-Is-my-account-and-credit-card-information-safe-.

More information on individual users' data security is available in five of the six Providers' existing user terms and conditions and privacy policies (see **Appendix B** and **Appendix C**). These documents are not yet available for Oakland Parking Solutions due to their app being a custom-build. However, all Providers will be required to comply with the terms included in the "City Data Addendum" (see **Appendix A**).

Regarding data retention, staff will require that Providers store only one (1) year of processed, anonymous data in their respective portals in order to provide sufficient time for parking citation appeal processes. Providers will store raw (unaggregated) 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 agreement to delete all raw parking payment transaction data collected in Oakland (see **Appendix A**). If such an event occurs, the Provider will be asked to email the DOT Project Manager a confirmation that all raw data collected in Oakland has been deleted.

8. Fiscal Cost

Providers operate at no direct cost to the City of Oakland. Instead, parkers who use the Providers' services pay a fixed fee to the Provider per parking session, in addition to the cost generated by the meter. Currently, parkers pay $0.25 per transaction *plus* the amount of time that they wish to park according to the meter rates.[7]

To adhere to generally accepted accounting principles (GAAP), the draft agreement requires that the City collect all revenues for all parties, including the Providers' user fees. As a result, Providers will invoice the City monthly to receive their user transaction fees. This practice is consistent with the existing agreement and practice with ParkMobile.

Staff are anticipating an increase in parkers using mobile parking payment services under the enhanced system and have thus allocated that up to $900,000 of user fees per year in the

[7] The Master Fee Schedule permits that meter rates may be adjusted between $0.50 and $4 per hour.

contract amount that will be reimbursed to the Providers. The Providers will only receive the reimbursed user transaction fees and will not receive any payment from the City. DOT staff have estimated a total of 14,000,000 transactions generated over the total contractual period across all Providers, including in the optional extension years. The contract amount has been set based off the maximum projected transactions per year (see **Table 1**).

Table 1: Estimated Parking Revenues and Transactions

	2019 Actual	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6 optional	Year 7 optional
Total Estimated Parking Revenue	$14.6 million	$15.3 million	$16.1 million	$16.9 million	$17.8 million	$18.6 million	$19.6 million	$20.5 million
Estimated Parking Payment by Phone/App	13.40%	16.75%	20.00%	25.00%	30.00%	35.00%	40.00%	45.00%
Estimated Average Transaction Amount	$2.57	$2.60	$2.65	$2.70	$2.75	$2.80	$2.85	$2.90
Total Estimated Transactions	761,443	987,606	1,214,830	1,564,938	1,935,970	2,329,214	2,746,021	3,187,810

Additionally, selected Providers will contribute to the City's expenses to operate and maintain the enhanced mobile parking payment system, including but not limited to installing signs and reconciling the system's funds. At the beginning of the contract term, each Provider will pay their designated portion of the one-time upfront "start-up" fee of $190,000. Each Provider will also share 10% of their user fee revenues generated in Oakland with the City on an ongoing basis.

Currently, the user fee is $0.25 per transaction with ParkMobile. The proposed user transaction fees for each selected Provider are below (see **Table 2**). In the enhanced mobile parking payment system, user fees are expected to be a primary point of competition between Providers for parkers' business and loyalty. Providers may also compete through their marketing efforts, such as first-time user promotional codes. Per the draft agreement, the City may choose to waive user fees at any time and instead pay them on behalf of the parker.

Table 2: Selected Proposers' User Transaction Fees

Provider	User Fee (per user transaction)
PayByPhone	$0.25
Passport	$0.20 *Note: may include gateway fee (+$0.05)
ParkMobile	$0.40
Honk	$0.25
Oakland Parking Solutions	$0.30
IPS	$0.25

9. Third Party Dependence

Raw (unaggregated) parking payment transaction data will be received and stored by the Providers on an ongoing basis. The City does not collect this data, nor does it have the means to store this data in compliance with industry standards. Most Providers, including the six selected Providers, rely on third party storage and/or security services. These detailed processes and services were provided in confidence in each Provider's proposal. However, third party authorization and use is broadly covered in five of the six Providers' privacy policies (see **Appendix B**). Because Oakland Parking Solutions is custom-building an app in order to operate in Oakland's mobile parking payment system, their privacy policy is not yet available for review.

10. Alternatives

The primary alternative to the proposed data sharing agreement is not enforcing any of the additional privacy or security features provided in the RFP. This may have reduced barriers to entry for Providers to Oakland's mobile parking payment system but would have resulted in a less secure mobile parking payment system. Because DOT staff received proposals from a range of Providers (large and small, local and not local) in the competitive process, this alternative may not have actually resulted in an "easier" proposal process for potential or existing Providers but certainly would have compromised the security of users' data in Oakland.

11. Track Record

Mobile parking payment services are available in cities throughout California, the United States, and the world. However, the City's 10 years of experience with mobile parking payment services is most pertinent to the purpose of this report. ParkMobile has been the City's Provider since 2011. In a typical year since 2015, about 10 to 15% (typically $1.5 to $2 million) of annual on-street parking payment transactions are made through ParkMobile. In addition to procuring a system with enhanced privacy and security measures, a key challenge with this service has been the maintenance of signage showing the zone number. Thus, a renewed investment in signage, including the initial start-up fee and ongoing revenue share, was a key component of the new system's RFP and innovative for the nature of this procurement.

In March 2021, ParkMobile experienced a data breach of over 20 million users' information. In an email sent by ParkMobile on April 13, 2021, DOT staff were notified of the following: "[Parkmobile's] investigation has confirmed that basic account information – license plate numbers and, if provided by the user, email addresses and/or phone numbers, and vehicle nicknames – was accessed. In a small percentage of cases, mailing addresses were affected. No credit cards or parking transaction history were accessed, and [Parkmobile does] not collect Social Security numbers, driver's license numbers, or dates of birth." In response to community members' concerns regarding the breach, DOT provided more information and resources about the breach on the City's website.[8] Staff did not discover any other reported data breaches from the other five Providers in their research.

Staff will not ask ParkMobile to migrate user information or data to the additional new Providers operating under the enhanced mobile parking payment system in order to avoid any compromise of the company's marketing and customer retention efforts. Rather, ParkMobile will now be competing with five (5) other Providers for parkers' business in Oakland. Providers will primarily compete through transaction fees and promotions but may also compete through their privacy policies and practices that enhance parkers' privacy.

The enhanced mobile parking payment system service supports the City's Parking Principles (Resolution No. 84664 CMS) by making parking easier and will be used as a pillar of the parking system. As cities increasingly move to multi-vendor mobile parking payment systems, the City continues to be on the forefront of innovation and data privacy standards through this next-generation mobile parking payment system. DOT staff are thrilled to be delivering a more secure system to parkers in Oakland that complies with the Surveillance Technology Ordinance and enacts the necessary mitigations to protect individual user data.

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

[8] This response is available here: https://www.oaklandca.gov/topics/parkmobile-march-2021-data-breach

ATTACHMENT A

DRAFT – CITY DATA ADDENDUM

This City Data Addendum [”Addendum”] is Exhibit 1 to the Professional Services Agreement between the City of Oakland [“City”] and [VENDOR’S NAME] [“Contractor”] to provide Mobile Parking Payment Services [“Agreement”] as is set forth with specificity therein and is incorporated into the Agreement by this reference. In the event of a conflict between the terms and conditions of this Addendum and the Agreement, the terms of this Addendum shall prevail but only with respect to the matters stated herein.

1. Background

As is set forth with specificity in the Agreement’s Statement of Work Exhibit [INSERT CITATION], Contractor avers and covenants to develop, implement and operate a mobile parking payment system [“System”] that, at a minimum, will enable customers to remotely pay for parking sessions by using mobile phones or mobile devices to provide Contractor payment information which Contractor will collect and store for City on Contractor’s mobile software application, website, and/or phone number for City-controlled paid parking [“Services”]. Contractor’s Services may also support daily or monthly permits by zone merchant validation

Given the sensitive nature of the information Contractor will collect and store for City, Contractor further avers and covenants that its System and Services will meet the City’s key goal of enhancing user data protections by complying with: (1) the City’s Surveillance Technology Ordinance (Oakland Municipal Code Chapter 9.64); (2) the City’s Surveillance Impact Report [Exhibit INSERT]; and, (3) the City’s Mobile Parking Payment Use Policy [Exhibit INSERT], all of which are incorporated herein by this reference.

ATTACHMENT A

2. Information to be Collected

The Agreement will require Contractor to collect from the users of its System, a broad range of personal and sensitive information. The California Consumer Privacy Act [CCPA][1] and Consumer Privacy Rights Act ["CPRA"] [2] definitions for "personal information"[3] and "sensitive personal information"[4] are incorporated herein by this reference and shall apply to the information Contractor collects.

3. Ownership of Information Contractor Collects

With the exception of that information which is publicly known or available as set forth in Section [INSERT] ["Confidential Information"] of the Agreement, all data, files, documentation, information, communications, media, whether intangible or tangible, whether provided directly or indirectly by Contractor to provide its Services, together with any and all results of Contractor's providing of its Services, including all data Contractor accesses , collects, modifies, develops as work product, or otherwise generates while providing its Services to City under this Agreement, whether pursuant or incidental to the purposes of the Agreement and whether or not delivered to the City, shall be the exclusive property of, and all ownership rights therein shall vest in, the City (collectively "City Data").

To the extent necessary, Contractor hereby assigns to the City, the rights to City Data which arise out of, or are developed in connection with or are the results of, Contractor's Services.

---

[1] Cal. Civ. Code Section 1798 *et. seq.*

[2] The CPRA is more accurately described as an amendment of the CCPA. The CPRA specifically states that it "amends" existing provisions of Title 1.81.5 of the California Civil Code (currently known as the CCPA) and "adds" new provisions (related to the establishment of the California Privacy Protection Agency).

[3] It 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.

[4] It contains some or all of the following;

- social security, driver's license, state identification card, or passport number
- account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.

ATTACHMENT A

4. Use of City Data

4.1 By Contractor

Contractor avers and covenants to:

- Comply with the terms of the City's Surveillance Technology Ordinance [OMC 9.64]
- Comply with
    - the City's Surveillance Impact Report [Exhibit INSERT CITATION];
    - the City's Mobile Parking Payment Use Policy [Exhibit INSERT CITATION],
- Anonymize the City Data and take such other steps as may be required to assure that personally identifiable or personally sensitive information are not visible to City staff at any time for any reason;
- Not sell rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, City Data, to another business or a third party for monetary or other valuable consideration;
- Only share City Data with third parties as permitted by City's Mobile Parking Payment Use Policy [Exhibit INSERT CITATION; Section 8 "Third-Party Data-Sharing"];
- Only use City Data to fulfill its obligations to City under the Agreement;
- Comply with the terms of the Agreement;
- Implement security safeguards;
- Not combine City Data with personal information received from others;
- Notify City when it uses subcontractors;
- Pass through the Agreement's terms and conditions to any subcontractors it uses;

.

Contractor shall fully indemnify City for any third-party claims against City resulting from Contractor's use of City Data in violation of this Addendum's provisions.

3.2 By City

City's access to City Data shall be limited to authorized staff and used only as permitted by City's Surveillance Use Policy [INSERT CITATION] and as required by City's parking enforcement responsibilities [INSERT CITATION]] which include but, are not limited to, shaping parking policies and practices to better support the City's Parking Principles and developing a more equitable mobility system. In this regard, only designated DOT and Finance Department staff will have access through unique portal credentials to the following *anonymized* City Data Contractor stores:

- Estimating parking demand, occupancy, and revenues;
- Evaluating parking payment options;
- Monitoring demand-responsive parking areas and compliance;
- Reconciling payment transactions with total parking revenues received;
- Promoting compliance and enforcing parking restrictions, permits, and payment;
- Reviewing contested parking citations;
- Remitting user transaction fees to Providers via invoices;

4. Contractor's System Security

This Agreement requires Contractor to store City Data in Contractor's certified data center[s] which are external to the City's premises and administered by Contractor for the purposes of this Agreement ["System"]. City's Data is highly sensitive, confidential and is of paramount importance to the City because unauthorized disclosures of the Data could seriously harm the City and possibly third parties.

Contractor acknowledges that City, in entering into this Agreement with Contractor, is relying upon Contractor's professional expertise, know-how, judgment, experience and its

representations in its System Security Plan [INSERT CITE TO VENDOR'S PLAN] that the integrity of the security, availability and processing of its System protects and preserves the confidentiality and privacy of the City Data. Contractor warrants that its System has been accredited under industry recognized standards [e.g., SOC 2] and that, at all times, Contractor will maintain and ensure that the Data remains secure and does not through any of Contractor's actions or lack of action thereof become vulnerable to unauthorized access by third parties.

Contractor avers and covenants to continue to take all technical and organizational measures necessary to protect the information technology systems and data used in connection with the operation of the Contractor's business. Without limiting the foregoing, Contractor will continue to use reasonable efforts to establish and maintain, implement and comply with, reasonable information technology, information security, cyber security and data protection controls, policies and procedures, including oversight, access controls, encryption, technological and physical safeguards and business continuity/disaster recovery and security plans that are designed to protect against and prevent breach, destruction, loss, unauthorized distribution, use, access, disablement, misappropriation or modification, or other compromise or misuse of or relating to any information technology system or data used in connection with the operation of Contractor's business.

Contractor agrees to maintain the City Data and to not disclose such information except as required to perform hereunder or as required by law.. Contractor shall maintain network risk and cyber liability coverage (including coverage for unauthorized access, failure of security, breach of privacy perils, as well at notification costs and regulatory defense) as required by the City's Schedule Q. Such insurance shall be maintained in force at all times during the term of this Agreement

Notwithstanding as may be otherwise provided in either this Addendum or this Agreement and, with the exception of those instances for which the City is responsible,

ATTACHMENT A

Contractor avers and covenants to be solely responsible for restoring and correcting any corruption to City's Data that occur by reason of Contractor's actions or lack thereof, including ransomware attacks upon Contractor and to fully indemnify the City for any claims against City and injury to City resulting from corruptions of the City Data.

5. DATA INCIDENTS

a. Contractor shall be responsible for managing the correction of unauthorized disclosure of, access to, or use of any City Data however they may occur ("Data Incidents").

b. In case of a Data Incident, or if Contractor confirms or suspects a Data Incident, Contractor shall: (1) promptly, and in any case within 24 hours, notify City by email, telephone, in person, or by other real-time, in-person communication; (2) cooperate with City and law enforcement agencies, where applicable, to investigate and resolve the Data Incident, including without limitation by providing reasonable assistance to City in notifying injured third parties; and (3) otherwise comply with applicable laws governing data breach notification and response.

c. In addition, if the Data Incident results from Contractor's other breach of this Agreement or negligent or unauthorized act or omission, including without limitation those of its subcontractors or other agents, Contractor shall (i) compensate City for any reasonable expense related to notification of consumers and (ii) provide 2 years of credit monitoring service to any affected individual.

d. Contractor shall give City prompt access to such records related to a Data Incident as City may reasonably request. City will treat such records as Contractor's Confidential Information pursuant to Section [INSERT CITATION TO CONFIDENTIAL INFORMATION OF THE CONTRACT WITH THE VENDOR] Contractor is not required to give City access to records that might compromise the security of Contractor's other users. City will coordinate with Contractor on the content of any intended public statements or required

notices for the affected individuals and/or notices to the relevant authorities regarding the Data Incident(s).

6. Termination of the Agreement

Within ten (10) days of the date of termination of the Agreement for any reason, Contractor shall send all City Data to City in a format acceptable to the City and which protects and preserves the sensitive nature of the City Data. Contractor may not keep copies of the City Data. For the purposes of this provision, Contractor's Assignment of the Agreement under Section [INSERT CITATION] ["Assignment"] or Bankruptcy under Section [INSERT CITATION] ["Bankruptcy"] of the Agreement or cessation of business shall be considered a Termination of the Agreement.

C. SCOPE OF SERVICES

The Consultant will be expected to provide the development, implementation, and operation of a mobile parking payment system that, at minimum, would enable customers to remotely pay for parking sessions using mobile phones or mobile devices through Consultant's mobile software application, website, and/or phone number for City-controlled paid parking. The City is also seeking, but is not requiring, services that support special permits (daily or monthly permits by zone) and merchant validation.

The mobile parking payment system provided by the Consultant shall be fully interfaced with the City's existing enforcement and citation management systems. The City's Parking Control Technicians must be able to view valid parking sessions made with the Consultant through their handheld devices. In demand-responsive parking areas of Oakland, the corresponding zone number must be visible in Parking Control Technicians' handhelds. In the case of an errant citation, the City must be able to check if parking sessions made through the Consultant have approved payment methods. Upon approval through the Consultant's system, valid parking session payment made through the Consultant must be received by the City and its financial system. All parking fees, including system and user fees, will be deposited into the City's bank account, then reimbursed to the Consultant.

The term of the awarded Agreement shall be for a base term of five (5) years, with two (2) consecutive one-year options to extend the term of the Agreement at the City's sole discretion. The mobile parking payment system(s) must be fully developed, implemented, and operational on the date specified in the awarded Agreement. Consultant shall be permitted to charge customers a single flat convenience/user fee per transaction for each use of the service. The convenience/user fee amount shall be approved in writing by the City. The City reserves the right to subsidize this convenience/user fee at any time during this agreement's duration. After the five-year base term of the agreement, selected Consultant(s) may request changes to the convenience/user fee amount. This request must be submitted in writing to the City of Oakland project manager or designated representative 90 calendar days prior to taking effect. The City of Oakland reserves the right to refuse a change to a Consultant(s)' requested change(s) to the convenience/user fee amount. Any changes to the convenience/use fee amount must be approved in writing by the City of Oakland in order for those changes to take effect.

The successful proposal(s) shall demonstrate that the Proposer(s) have the appropriate professional and technical background as well as access to adequate resources to fulfill the scope of services, as outlined in Tasks 1 and 2 below. The City may select multiple qualified Proposers for the mobile parking payment system (Task 1). Proposer(s) may also choose to respond to Task 2, if the Proposer has additional services or products that can effectively support the on-street and off-street parking system.

TASK 1 Mobile Parking Payment System

1.1 Technical Requirements and System Integration. The system must perform key technical functions and have full integration capabilities with the City's existing systems. The following system requirements must be met at no cost to the City of Oakland, as only the convenience/user fees applied be invoiced by the awarded Consultant(s):

- Integrate with the City's current parking citation processing system (Conduent's eTIMS®) and accommodate any future potential changes to the system.
- Integrate with current parking enforcement handhelds (Zebra TC75X) and Automated License Plate Readers (Genetech's AutoVu) and accommodate any future potential changes to parking enforcement equipment.
  - For context, City of Oakland Parking Control Technicians conduct enforcement queries by zone up front and double check for payment at the end of the ticket-writing transaction to confirm a payment has been made.
- Integrate with digital payment technology and IPS single- and multi-space meters, should the City decide to "push" mobile payments to meters.
- Integrate with any other parking data, payment, and management systems and platforms that the City may acquire during the Consultant(s) operation.
- Display the status of paid vehicles on any Internet browser, in real time, through a secure portal requiring unique credentials for each staff with access.
- Provide the ability to cross-reference transactions between vehicles, individual meters, streets, block, zone, or other designated identifiers.
- Provide the ability to geographically depict/map parking transaction activity.
- Provide real-time transaction information in the form of printable reports (such as through an online portal/back-office system) and accessible through enforcement handheld devices for purposes of enforcement and verification/audit of real-time push to IPS smart meters.
- Integrate payment zones with the City's selected number typology.
- Provide the capability for the City, instead of parkers, to pay transaction fees on an as-needed basis, such as for a district-specific holiday promotion.
  - This capability should include a pop-up or notification to customers that the City of Oakland is covering user fees. Consultant(s) shall be able to provide this capability citywide or in specific zones upon the City's request and may recommend zones/districts where this promotion would be beneficial to parkers, such as where there is low mobile parking payment adoption.

1.2 Point of Service. The system must provide key points of service to parking customers. The system must allow customers to perform the following functions:

- Create an account/register via mobile smartphone app, over the phone through an automated system, and over the Internet via mobile and desktop web with minimal input requirements (basic information) and be able to immediately begin using account.
- Other registration options/platforms are encouraged but not required (Facebook, etc.).

- Start a parking transaction and make payment via smartphone software application, Interactive Voice Response (IVR), Short Message Service (SMS), or website.
- Be alerted automatically via text prior to a parking session expiring.
- Extend a parking session and purchase additional time within established time parameters via smartphone software application, IVR, SMS, or over the internet via mobile and desktop website.
- Extend a parking session without re-entering complete location information.
- Extend a parking session without incurring additional convenience/user fee.
- Initiate a new parking session at a previously parked location without re-entering information.
- Prepay for parking during a designated "prepayment period."

1.3 System Setting Requirements. The system must include unique settings that permit the following functions:

- Utilize and display City-created block ID numbers containing up to eight (8) alphanumeric characters for payment zones.
- Allow settings to vary at each individual meter, by block, by zone, by time, by restriction, and by other custom configurations/groupings.
- Allow custom settings to define and/or modify maximum stay restrictions.
- Allow the programming of multiple, custom, and variable rate structures by time of day, day of week, hours of operation, length of stay, by individual meter, by zone, and by other custom configurations/groupings.
- Allow custom, unlimited configuration changes related to rates, hours of operation, and time limits to be programmed in advance with the ability to be active within two (2) days of the programming change. All other system configuration changes/updates shall be made within five (5) days of notification.
- Have the ability for Consultant to change parking session rates to support the City's demand-responsive parking program. Consultant should specify in how many business days they are able to adjust rates and for rates to be available with the system.
- Disallow parking transactions to be initiated on City designated holidays or during periods designated by the City as no parking.
- Allow for custom grouping of meters to facilitate enforcement, revenue reporting, and demand-responsive parking rate programming.
- Enable City staff to add, remove, or alter meters or spaces within the pay-by-phone system inventory.
- Allow for the deactivation or suspension of a customer account in the event that a parking payment transaction is declined three (3) times and provide notification to customer of such action.
- Allow City staff to access up to two (2) years of data in the Consultant's online portal/back-office system.
    - If the contract between the Consultant and DOT is severed, the Consultant will be required to delete all raw parking payment transaction data collected in Oakland.

- Provide an online system portal/back-office system that includes parking date and start and end times, payment amounts, transaction fees for the Providers, and numbered "zones" corresponding to parking location.
- Incorporate the latest Americans with Disabilities Act (ADA) Guidelines and best practices for accessible digital content, including but not limited to Section 508.

1.4 Data Privacy Requirements. One of the key goals of this new pay-by-phone system is to enhance user data protections. The system must comply with the City's Surveillance Technology Ordinance (Oakland Municipal Code Chapter 9.64) and subsequent system use policy and anticipated impact report[1] in the following capacities:

- Maintain an online system portal/back-office system with **none** of the following information visible to staff at any time for any reason:
  - Personally identifiable information (PII), such as phone number and email address
  - Customer license plate information (note: this information must be visible for real-time enforcement purposes, but not to office staff accessing the online portal)
  - Individual user account details
- Provide a system with data security, storage, and encryption practices that meet or exceed industry standards. DOT expects that these best practices will primarily address user payment methods to protect credit card information.
- Disclose any additional companies who would support the Consultant's system, such as third-party cloud storage services.
- Ensure the security of user and transaction data through security protocols per current industry standards.
- Provide a data storage and privacy system that meets or exceeds industry standards. Consultant must comply with the City's Surveillance and Community Safety Ordinance (Oakland Municipal Code Chapter 9.64), the approved policy use regarding the mobile parking payment system, and any other relevant surveillance laws relevant to Oakland, California.

1.5 Customer Base System Requirements. The system must support customer transactions and should provide a positive customer experience. The system must allow the following functions:

- Provide a toll-free live customer service telephone support for all aspects of the pay-by-phone system.
- Allow customers the option to transfer to a live customer service agent at any time when utilizing an automated system.

[1] These documents will be made available on the City's website: oaklandca.gov/topics/approved-impact-reports-and-use-policies

- Allow customers the ability to manage, modify and track account details, update settings and profile, review usage, view transactions, and print receipts via the smartphone software application and over the internet via mobile and desktop web.
- Allow customers the ability to designate multiple vehicle license plates to a single account.
- Provide customers email receipts of all parking transactions.

1.6 Payment System Settings. The system must permit the following functions to support customer payments, parking system management, and parking payment reconciliation and audits:

- Include all applicable convenience/user fees assessed to users.
- Notify customer of any convenience/user fees to be charged regardless of payment type/option utilized.
- Provide revenue, utilization, and other reports in a format exportable to Excel, allowing for easy data analysis, record keeping/documentation, and reconciliation.
- Provide a secure gateway service for secure (encrypted) credit card data transmission to the City's merchant account provider. Credit card data transmission shall meet the Payment Card Industry Data Security Standards (PCI DSS) Level 1 certification.
- Authorize payments in real time and accept payment through Visa, MasterCard, Discover, American Express, all debit cards, and other alternate payment methods (i.e. PayPal, Apple Pay, Google Pay, Venmo, etc.).
- Document for review and report rejected/declined transactions to the customer.
- Provide a single opportunity for customers to try a different credit or debit card when a rejected transaction occurs.
- Ensure declined transactions are not incorrectly posted within the revenue reporting system or pushed to the meter.
- Synchronize batch settlement times for the merchant account and report of the same sent via the Internet to the City.
- Have expansion capacity and state how much expansion capacity the system has in terms of spaces, meters, or any other defined criteria.
- Have the capability to implement parking validation, such as allowing merchants to generate and provide customers with unique discount codes.
- Provide a fully auditable service and online portal/back-office system for as-needed audits conducted by City staff, in addition to complying with PCI DSS audits.

1.7 Informational Materials and Promotion. The system must include informational materials and the promotion of the City's integrated mobile parking payment system, such as through the use of stickers, decals, and/or signage and online promotions. All materials in the public right-of-way will be Oakland-branded and connect parkers to an Oakland-branded website. The website will direct parkers to all permitted Consultants, such as by showing individual Consultant logos and links to their platforms.

While the City will install and maintain informational materials, such as City-branded

parking signs, in the public right-of-way, Consultant(s) shall pay for the cost of these activities through both an initial fee and ongoing revenue sharing of user/transaction fees paid to the City. The City is committed to promoting the use of this new system and is seeking financial support from Consultant(s) to fully execute this commitment and ensure Oakland parkers' access to their services.

The City is seeking an initial one-time combined payment of $190,000 from all selected Consultant(s) to contribute to the costs of establishing the new mobile parking payment system. $190,000 shall be divided equally between all selected Consultant(s), unless otherwise specified or unless the Consultant(s) is a certified LBE. If the Consultant(s) is a certified LBE, then this Consultant(s) shall contribute 75% of their divided portion.

Unless otherwise determined in negotiation, selected Consultant(s) shall pay: 1) their agreed-upon portion of $190,000 one-time fee to the City at the beginning of the agreement term and 2) 10% of all convenience/user fees collected shall be kept by the City of Oakland.

The system must include the following materials and promotion:

- Contribute toward the cost to install City-branded signage for paid parking areas. Consultant must propose a certain annual percentage of transaction, user, and/or gateway fees that they will commit to a City account dedicated to installing, maintaining, and replacing parking signs, stickers, and/or decals.
- Provide funding for Oakland-branded materials to promote the mobile parking payment system that will be displayed in the public right-of-way and online. Materials shall include but are not limited to signs, stickers, and decals.
    - Materials must show individual zone numbers and a link to the City's website page on available mobile parking payment system(s). City will approve final stickers, decals, and signs prior to the Consultant's' installation.
    - Signage proposals shall meet the City's requirements/specifications for signage design, manufacturing, and maintenance.
- Support City staff in connecting parkers to the Consultant's product on the City's online Oakland-branded platform. Support may include but is not limited to links that open Consultant's smartphone software applications or website and official Proposer logos provided as .png or .jpg images.
    - Provide City staff with digital informational or marketing materials, such as promotions to include on the City's mobile parking payment system website (e.g., a digital coupon code for new sign-ups on the Proposer's app) and instructions on how to use the Consultant's product.

1.8 System Set-up and Training. The system set-up shall be without cost to the City and must include but not be limited to the following functions:

- Supply reports for account sign-up and use, customer service issues, revenue, and

additional reports deemed necessary by the City to properly evaluate program progress.
- Describe reporting options in their response including whether reports can be customized.
- Provide on-site or web-based training and manuals for the authorized City personnel to navigate and utilize the online portal/back-office system.

1.9 Community Benefit and Engagement. Consultant(s) staff shall maximize the benefits of their pay-by-phone system to Oakland parkers by engaging directly with community members and organizations. Methods of engagement will include, but not be limited to, the following:

- Attend up to four (4) community events per year either in-person or virtual, such as business improvement district (BID) meetings, Oakland City Council or commission meetings, and neighborhood events.
  - Two (2) or more of these events must occur in Equity Priority Communities, as defined by the Metropolitan Transportation Commission, as shown here: https://mtc.maps.arcgis.com/apps/mapviewer/index.html?layers=28a03a46fe9c4df0a29746d6f8c633c8
- Incorporate community feedback into Proposer's product functionalities, promotions, marketing materials, and system.
- Align Proposer's goals for their product in Oakland with community goals, such as goals formed in the Proposer's collaboration and outreach with community members and goals stated in OakDOT plans to promote a sustainable, equitable and livable city.

Task 1 Deliverables:

- *Fully integrated and set-up parking payment system that meets all technical requirements, permits all points of service to the public, meets setting and customer base requirements, includes all payment system settings, and provides informational materials and promotion.*
  - *Informational materials and promotion including but not limited to stickers, decals, and signage installation.*
  - *Web-based trainings and manuals for authorized City personnel to navigate and utilize the online portal/back-office system.*
- *Attendance and support at up to four (4) community events per year, either in-person or virtual.*

TASK 2 (OPTIONAL) Additional Parking System Support

In addition to providing a mobile parking payment system, Proposer(s) may choose to include additional innovative products or services for the City's consideration. These products or

services should support the active management of the City's parking system, supporting access to commercial areas and curbside spaces, and integrating off-street facilities into the City's on-street system.

Task 2 Deliverables:

- *Innovative product(s) or service(s) that supports the parking system.*
    - *Examples of such products or services may include: pay-by-text parking payment, gateless parking system technologies, integrated pay-by-phone services for Proposer(s), commercial vehicle parking permits, integrated enforcement features, and equitable cash payment alternatives.*
    - *Product or service should include detailed pricing, technical requirements, named benefits to Oakland's parking system, other municipalities or organizations where the product or service is in use, and any other relevant information.*

D. DELIVERABLES

Deliverables listed below shall provided to the City per a timeline agreed upon by City and the Proposer. Request for information or reports shall be fulfilled by the Proposer within three (3) business days of the request.

Task 1 Deliverables:

- *Fully integrated and set-up parking payment system that meets all technical requirements, permits all points of service to the public, meets setting and customer base requirements, includes all payment system settings, and provides informational materials and promotion.*
    - *Informational materials and promotion including but not limited to stickers, decals, and signage installation.*
    - *Web-based trainings and manuals for authorized City personnel to navigate and utilize the online portal/back-office system.*
- *Attendance and support at up to four (4) community events per year, either in-person or virtual.*

Task 2 Deliverables:

- *Innovative product(s) or service(s) that supports the parking system.*
    - *Examples of such products or services include: pay-by-text parking payment, gateless parking system technologies, and equitable cash payment alternatives.*
    - *Product or service should include detailed pricing, technical requirements, named benefits to Oakland's parking system, other municipalities or organizations where the product or service is in use, and any other relevant information.*

SMARTER PARKING for SMART CITIES™

PRIVACY POLICY

Privacy Statement

IPS companies and locations

- Headquarters: 7737 Kenamar Court, San Diego, CA 92121, U.S.A

- United Kingdom: International Parking Systems (UK) Ltd., Railway Court, Doncaster, DN4 5FB, United Kingdom
- IPS Europe SRL: Via P. Carnerini 1/A, 43123, Loc, Pilastrello (PR) Italy

Company Websites

https://ipsgroupinc.com
https://ipsgroupinc.co.uk
https://ipsgroupsrl.eu

Web & Mobile Apps

https://www.myparkingreceipts.com
https://www.myparkingreceipts.co.uk
https://www.parksmarter.com
https://ipsenforcement.com
https://thepermitportal.com
https://ce.ipsenforcement.com
https://ipspermits.com
https://citationportal.com
https://civilcites.com

When This Statement Applies

IPS is a group of affiliated design, engineering, and manufacturing companies focused on low-power wireless telecommunications, payment processing systems, parking technologies, parking enforcement and management SaaS software. IPS is headquartered in the United States and operates globally, with affiliate companies in other countries including Canada, United Kingdom, Ireland and Italy. This privacy statement applies to IPS, Inc. and its affiliates below indicated (“IPS,” “we” or “us”). IPS is responsible for the processing of personal information – information about you that can directly or indirectly identify you personally – that you provide when you interact with any IPS company on its web sites (“Sites and Services”), mobile applications, other technologies described in this Privacy statement and any other sites or services under our control where this Privacy Statement is displayed. The data controller of ipsgroupinc.com and data collected by IPS through its web sites and

business operations is IPS Group, Inc. This Privacy Notice describes how we collect, receive, use, store, share, transfer, and process your personal information, as well as your rights in determining what we do with this information.

Note that IPS also collects and uses personal information on behalf of its public and private organization customers as it provides them services. In these cases, IPS operates only on directions of these customers and the privacy statements of those organizations apply.

For example, we sell parking meters to cities, universities, and other public and private parking site operators. We also provide on-going services to assist these organizations in parking payment processing, payment refunds, and parking enforcement and tracking. In these cases, we are the service provider to these organizations and collect and use end user personal information at their direction for the limited purpose of providing the service for which our client has engaged IPS.

Personal Information We Collect and How We Use It

IPS may collect information from and about you when you visit our web sites, set up an account with IPS or use our mobile applications, or interact with us. The following are brief descriptions of the information we may collect and how we use it.

Mobile / Web Application Registration and Service Data

Many of IPS services are offered to business and governmental customers, in which case IPS is a service provider to those customers and this privacy statement does not apply. However, if you register for one of our mobile applications that we offer directly to end users like you, such as ParkSmarter and MyParkingReceipts, either through a web site or on your mobile device, IPS is the controller of the data and this privacy statement applies. Through your registration and our application(s) we may collect your name, email address, telephone number, username and password,

vehicle information such as: make, model, color, year, license plate number, and state, and for payment processing we collect payment and credit card information. As you use these services we may also log and maintain your usage and transaction data, and we collect and process your payment information. We use these data to fulfill and improve your service, respond to your requests, and with legitimate business interest, to understand and enhance our products and services. We may use your personal information to fulfill legal obligations and protect our legal interests. With your consent, we may also use your name and contact information to market to you.

If you request services that require geolocation, such as functionality to find available parking spots near you, we will ask for your explicit consent to turn on GPS geolocation for our application during the consent process provided by your device. We only use this information to provide your requested service, and you can withdraw your consent at any time through your mobile phone location service settings.

Product Improvement and Testing Data

In an effort to improve our products and services, and help ensure accuracy of sensors and equipment, from time to time in the United States we perform camera audits of our parking meter activities for our legitimate business interests. These camera audits involve taking photos of parking spots at regular intervals to validate parking meter accuracy involving parking spot vacancy status. These photos may capture vehicles and/or people when those vehicles or people occupy a parking spot being audited. We only use this information to validate accuracy of our equipment and do not log license plate numbers outside of the photo itself.

Web Site Data

We process personal information about you that we collect either directly, through forms or data entry fields on our website that you would voluntarily fill out, through log files that show us how you use our websites and applications, or through passive collection by cookies and

other data collection technologies. We use this information to fulfil your requests, provide service, improve our business and operations, and with your consent may market to you. For our legitimate business interests pertaining to security and fraud prevention, we may also collect and use information provided through cookies and other data collection technologies.

The types of personal data we process in each of these contexts is further explained in the following categories:

- Contact us and registration forms: We process your name, email address, company where you work, phone number, job function, job title, country, and any comments you provide. We use this information to fulfil your request, manage your service and our relationship, and with your consent send you messages about products and services that may interest you.
- Cookies and other data collection technologies: We and our service providers use technologies on our sites and services to collect information that helps us improve the quality of our sites and services and the online experience of our visitors and users. In this Privacy Notice, we refer to these technologies, which include cookies–small text files stored on your computer or mobile device to remember your actions or preferences over time, such as web beacons to help deliver cookies and gather usage and performance data, Local Storage, Javascript, eTags, and similar technologies from third party providers, collectively as "cookies." Most web browsers support cookies, and users can control the use of cookies at the individual browser level. Please note that if you choose to disable cookies, it may limit your use of certain features or functions on our sites and services.

We (and service providers on our behalf) use cookies and similar technologies to:

- Maintain or analyze the functioning of the website or online services
- Authenticate users of, or personalize the content on, the website or online service
- Protect the security of integrity of the user, website, or online service
- In the US to conduct marketing

We use browser session cookies, which are temporary cookies that are erased from your device's memory when you close your Internet browser or turn your computer off, and persistent cookies, which are stored on your device until they expire, unless you delete them before that time. In some countries, such as countries in the European Union, we provide a mechanism through which you can manage your cookie preferences – our "Cookie Preferences" manager. If this Cookie Preferences manager is available in your geography, you can select your preferences by clicking on the Cookie Preferences link at the bottom of the browser web page. If it is not available in your geography, you can opt out of cookies through your browser privacy settings.

Generally, our cookies fall within one of three categories:

- *Required cookies*: These cookies are necessary to enable the basic features of this site to function, such as allowing images to load or allowing you to select your cookie preferences.
- *Functional cookies*: These cookies allow us to analyze your use of the site to evaluate and improve our performance. They may also be used to provide a better customer experience on this site. For example, remembering your log-in details or providing us information about how our site is used.
- *Advertising cookies: Third-party advertisers and other organizations may use their own cookies to collect information about your activities on our sites and services and/or the advertisements you have clicked on. This information may be used by them to serve advertisements that they believe are most likely to be of interest to you based on content you have viewed. Third-party advertisers may also use this information to measure the effectiveness of their advertisements. We do not control these cookies and to disable or reject third-party cookies, please refer to the relevant third party's website.*

Software development kits: Our mobile applications contain software development kits (SDKs) that may collect and transmit information back to us or third-party partners about your usage of that mobile application or other applications on your device.

Flash cookies: Videos and other features on our site use Flash cookies to collect and store your preferences, such as volume. Flash cookies are different from browser cookies because of the amount of, type of, and way that data is stored. Cookie management tools provided by your browser will not remove Flash cookies. To learn how to manage privacy and storage settings for Flash cookies click here. Some cookies may be placed by third party service providers who perform some of these functions for us.

Server log files: We automatically gather server log file information when you visit our web sites. This includes IP address, browser type, referring and exit web pages, and your operating system. We use this information to manage security and prevent fraud and manage and improve our web sites and applications.

Cookie Preference Manager: As described in this Privacy Notice, IPS and third parties on our digital propert(ies) may use cookies and similar tracking technologies to collect information and infer your interests for interest-based advertising purposes. If you would prefer to not receive personalized ads based on your browser or device usage, you may generally express your opt-out preference to no longer receive tailored advertisements. Please note that you will continue to see advertisements, but they will no longer be tailored to your interests.

To opt-out of interest-based advertising by participating companies in the following consumer choice mechanisms, please visit:

- Digital Advertising Alliance (DAA)'s self-regulatory opt-out page http://optout.aboutads.info/ and mobile application-based "AppChoices" download page https://youradchoices.com/appchoices
- European Interactive Digital Advertising Alliance (EDAA)'s consumer opt-out page https://youronlinechoices.eu

In the mobile environment, most mobile operating systems offer device-based opt-out choices that are transmitted to companies providing interest-based advertising. To set an opt-out preference for a mobile device identifier (such as Apple's IDFA or Android's GAID), visit the device manufacturer's current choice instructions pages, or read more about

sending signals to limit ad tracking for your operating system here: https://www.networkadvertising.org/mobile-choices.

Please note that these settings must be performed on each device (including each web browser on each device) for which you wish to opt-out, and if you clear your cookies or if you use a different browser or device, you will need to renew your opt-out preferences.

Job Application and Hiring Data

If you apply to work at IPS, we process the resume and contact information you give us and information we may gather about you (reference and previous employer responses about your history, background checks) to review your suitability for the job to which you have applied. For our legitimate interests, we may retain your resume to determine your eligibility for future or other current positions. You can ask that we delete your resume at any time.

We collect information about you and your professional experience, education and training; such as your application/CV, your name (and any former names), postal address, email address, phone number, universities attended, academic degrees obtained, grades, professional certifications and licenses, employment history, and curriculum vitae or resume to evaluate your suitability to open positions.

Prior to making an offer of employment or a contractor position, we process personal information to conduct professional reference checks in accordance with applicable laws. If we extend an offer of employment or a contractor position at IPS to you, we will process personal information about the position to which you have been appointed, your job title at IPS, the compensation or project-based contractor rate we offer to you, your signed offer acceptance, and your starting compensation or project-based contractor rate, and your start date.

After you are hired but prior to commencement of your employment with us, we may engage service providers to conduct background checks that involve the necessary personal information processing as permitted by the laws in the location in which you reside and/or work. More details are

provided to you in the context of our request to you to complete these checks.

Marketing Data

We may use, for our legitimate interests, your name, email, telephone number, job title and basic information about you and where you work (name, address, and industry), as well as an interaction profile based on prior interactions with us to keep you up to date on the latest product announcements, updates, special offers, and other information about our services and events. This can be in the form of direct marketing email/phone calls and/or newsletters. We may also provide a hashed user ID to third party operated social networks or other web offerings (such as Twitter, LinkedIn, Facebook, Instagram or Google) where this information is then matched against the social networks' data or the web offerings' own databases in order to display to you more relevant information. If you no longer wish to receive marketing-related emails from us on a going-forward basis, you may opt-out of receiving these communications by clicking the unsubscribe button located in the footer of the email.

Information Related to Our Business Dealings Together

If you work for an organization that does business with us, we may use your business contact information (name, email address, phone number, and company postal mail address) to communicate about your organization's services and business relationship, assist with returns and maintenance authorizations (RMA), respond to your customer support requests, answer your questions, and otherwise manage our relationship and business together. For our legitimate interests, we may also communicate with you about products and services we believe may interest you.

If we meet you at a trade show or other event, or if you are a participant in such an event, with your consent we may use the business contact information you provide for marketing. If you have asked us to respond to

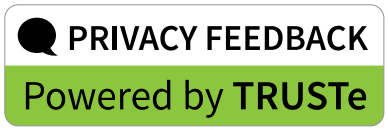
a question or request, we will use the contact information you provide to respond to your question or request.

If you visit our facilities, we may capture your image on security cameras and your contact information through our badging process for our legitimate business interests related to security.

Children

All IPS products and applications (services) are intended for adults. We do not intentionally or knowingly collect, personally-identifiable information from children under the age of 16 and we request that individuals under the age of 16 not submit any personally identifiable information to our services.

If you become aware that a child has provided us with personally identifiable information, please contact IPS at privacy@ipsgroupinc.com to allow us to remove any and all information relating to that child.



EU-U.S. Privacy Shield Program

Where We Store and Process Your Data

IPS is a global company and processes personal data in multiple locations around the world. Regardless of location, we provide a similar level of protection to personal data. For more information about the location of your data, contact us at privacy@ipsgroupinc.com. We are a participant in the EU-U.S. Privacy Shield program.

We may transfer, access, or store personal information about you outside of the European Economic Area ("EEA"), or another country that requires legal protections for international data transfer. When we do, we will ensure that an adequate level of protection is provided for the information by using one or more of the following approaches:

- Where personal information is transferred from International Parking Systems (UK) Ltd to IPS group Inc. headquarters in the USA, this transfer is subject to a contract between IPS UK and IPS Group that requires IPS Group to provide the same level of protection for the data as applies in the UK. In addition, IPS Group in the USA is fully certified as Privacy Shield compliant with the rules and requirements of that scheme.
- We may transfer personal information to countries that have privacy laws that have been recognized by the country from which the data are transferred as providing similar protections for the data.
- We may enter into written agreements with recipients that require them to provide the same level of protection for the data.
- We may rely on other transfer mechanisms approved by authorities in the country from which the data are transferred.

IPS Group, Inc. participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework.

IPS Group, Inc. is committed to subjecting all personal data received from European Economic Area and the United Kingdom in reliance on the Privacy Shield Framework, to the Framework's applicable Principles. To learn more about the Privacy Shield Framework, visit the U.S. Department of Commerce's Privacy Shield List.

IPS Group, Inc. is responsible for the processing of personal data it receives, under the Privacy Shield Framework, and subsequently transfers to a third party acting as an agent on its behalf. IPS Group, Inc. complies with the Privacy Shield Principles for all onward transfers of personal data from the European Economic Area and the United Kingdom, including the onward transfer liability provisions.

With respect to personal data received or transferred pursuant to the Privacy Shield Framework, IPS Group, Inc. is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, IPS Group, Inc. may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

How We Retain and Share Your Information

We do not sell or rent personal information to third parties for their own purposes, and we do not share personal information with third parties that are not owned by us or under our control or direction except as described in this privacy statement. We may share your information within the IPS group of companies. We may share your information with service providers under contract to us, as required by law, to promote safety and security/prevent fraud/protect our rights, in the case of a potential merger/acquisition/divestiture/asset sale.

- Within Our Corporate Family. We disclose PI to affiliated companies related by common ownership or control within the IPS Group of Companies to carry out regular business activities, such as to provide, maintain and personalize our sites and services, to communicate with you, and to accomplish our legitimate business purposes, pursuant to contractual safeguards.
- Service providers. We share personal information with service providers that helps us with our business activities. They only are authorized to process that information as necessary and as directed by us, pursuant to written instructions. In such cases, these companies must abide by our data privacy and security requirements.
- Required by law. In certain situations, we may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements. We may also disclose your personal information as required by law, such as to comply with a subpoena or other legal process, when we believe in good faith that disclosure is necessary to protect our rights, protect your safety or the safety of others, investigate fraud, or respond to a government request.
- Safety, fraud prevention, government requests and protection of our rights are all reasons where we may share personal information where we believe in good faith it is necessary.
- Corporate Transactions. If IPS is involved in a merger, acquisition, dissolution, sale of all or a portion of its assets, or other fundamental corporate transaction, we reserve the right to sell or transfer your

information as part of the transaction. In such an event, you will be notified via email and/or a prominent notice on our website of any change in ownership, incompatible new uses of your personal information, and choices you may have regarding your personal information.

Security and Data Retention

We take appropriate security measures to protect personal information against loss, misuse, and unauthorized access, alteration, disclosure or destruction. We also have implemented commercially reasonable technical and organizational safeguards to maintain the ongoing confidentiality, integrity and availability of the systems and services that process personal information and will restore the availability and access to data in a timely manner in the event of a physical or technical incident. IPS Group understands the importance of good information security and data stewardship, illustrating compliance through its certification to the Payment Card Industry (PCI) Data Security Standard. IPS develops, implements and sustains a wide range of policies, processes, procedures, and technical controls to keep your data secure.

Transmissions over the Internet are never 100% secure or error-free. However, we take reasonable steps to protect your personal information from loss or misuse, and unauthorized access, disclosure, alteration, and destruction. It is your responsibility to safeguard any password and User ID you use to access the site and to notify us through helpdesk@ipsgroupinc.com if you ever suspect that this password or User ID has been compromised. You are solely responsible for any unauthorized use of the site conducted via your password and User ID.

We will retain your Personal Information for the period necessary to fulfill the purposes outlined in this Privacy Notice and according to our internal data retention policy, unless a longer retention period is required or

permitted by law. For more information about how long we retain your data and where, contact us at privacy@ipsgroupinc.com.

Your Rights

Depending on applicable laws and with some limitations, you may have rights to ask that we give you access to, correct or update if inaccurate or incomplete, or delete, provide you copies of, or ask that we limit our uses and sharing of your personal information. You can also ask to be informed which third parties have had access to your personal information and in some cases ask to opt out of that sharing. If you object to how we have used your personal information, you can contact us to resolve the issue, and you also have the right to complain to a regulator. We will never discriminate against you for requesting any of these rights. To contact us about any of these individual rights, opt out of marketing or to express a complaint, contact us through:

Online Form: Click here to exercise your rights

Postal Mail: “Data Protection and Privacy” at IPS Group Inc, 7737 Kenamar Court, San Diego, CA 92121

Phone: 877-630-6638

Please note that for personal information about you that we have obtained or received for processing on behalf of a customer of IPS which determined the means and purposes of processing, all such requests should be made to that entity directly. Any direct inquiries received will be forwarded to the respective IPS customer for response.

We will honor and support any instructions the customer provides to us with respect to your personal information.

At any time, you can ask us what personal information we process about you and with which third parties we have shared it. You can also request a correction or deletion of your personal information. Note that we may delete your personal information only if we have no statutory obligation or prevailing right to retain it. Also, if we delete data that is required to use our services, you may not be able to continue to use those services.

If we use your personal information based on your consent or to perform a contract with you, you may further request a copy of the information you have provided us. You may also ask that we forward your information to a third party on your behalf.

You can request that we limit or stop processing your personal information if you:

- Believe it is incorrect,
- There is no legal basis for us processing it, or you
- Object to us processing the data based on our legitimate interest.

If you do make one or more of these individual rights requests, we will do our best to fulfil the request in a timely manner (usually within 30 days) and in accordance to legal requirements and our internal policies. Depending on the request, we are obligated to validate your identity before fulfilling that request.

If you believe that we are not processing your personal information in accordance with this privacy statement or your rights, contact us directly at privacy@ipsgroupinc.com to give us the opportunity to resolve the issue. You also can lodge a complaint with the data protection authority of the country in which you live or with the data protection authority of the country or state in which we have a registered seat.

Sale of Personal Information

Third Party Cookies

Third-party advertisers and other organizations may use their own cookies to collect information about your activities on our sites and services and/or the advertisements you have clicked on. This information may be used by them to serve advertisements that they believe are most likely to be of interest to you based on content you have viewed. Third-party advertisers may also use this information to measure the effectiveness of their advertisements.

These disclosures may be deemed as a 'sale' under the CCPA if such disclosure is for any valuable consideration, even if we do not receive any payment or discount. You can opt out of this sharing through third party cookies at the top of this page, or here.

Other Third-Party Sharing

Do not worry – we do not otherwise sell your personal information for payment or discount. We do not and have not sold any personal information in the preceding twelve months. This fact notwithstanding, you may have the right to opt out of any sale of your personal information.

If you do not want us to sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, your personal information to another business or a third party for monetary or other valuable consideration,

Please:

Submit a Do Not Sell My Personal Information request via the IPS Online Form.

Effective Date, Amendments

This statement is effective as of June 11th, 2021. We reserve the right to change this statement from time to time and in our sole discretion. We reserve the right to change, modify, add or remove portions of this statement at any time, but updated if we propose to make any material changes, we will notify you by direct communication and, or highlighting the changes on our website prior to the change becoming effective. When you visit the site, you are accepting the current version of this statement as posted on the site at that time. We recommend that users revisit this statement on occasion to learn of any changes.

Questions or Complaints

In compliance with the Privacy Shield Principles, IPS commits to resolve complaints about our collection or use of your personal information. Individuals with inquiries or complaints regarding our Privacy Shield Policy

and practices should first contact us by sending an email to privacy@ipsgroupinc.com.

If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request.

Binding Arbitration Under certain conditions, more fully described on the Privacy Shield website, you may be entitled to invoke binding arbitration when other dispute resolution procedures have been exhausted.

If personal information about you is transferred by IPS Group Inc. the EEA to the U.S. pursuant to Privacy Shield, and you have an unresolved concern regarding personal information processing about you that we have not addressed to your satisfaction, please contact the EU authorities at http://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.html.

Contact

Please feel free to contact us with any comments, questions, complaints or suggestions you might have regarding the information practices described in this statement.
You may contact us electronically at privacy@ipsgroupinc.com.
You may contact us in writing by sending letters addressed to “Data Protection and Privacy” at:
IPS Group Inc, 7737 Kenamar Court, San Diego, CA 92121.

Updated June 11th, 2021.

- Payment Processing
- Mobility Platform

- Transportation Software
- Curbside Management
- Smart Cities
- Open Ecosystem

We're committed to your data privacy.

Updated May 2020

Passport is committed to protecting the privacy of our clients and our users. When we facilitate transactions on behalf of our clients (cities), we act as their trusted agents, collecting for them only the aggregated and anonymized data they requested. This data helps our clients deliver beneficial outcomes including improved urban planning, congestion relief and easy access to parking.

When Passport facilitates transactions, users agree to provide information such as name, email and phone number so that Passport can deliver parking, permitting and transit services. Passport can also use this information to provide useful notifications, for example, when a parking session is about to expire or a permit needs to be renewed.

We protect personal information

- We understand that any data we collect must be used carefully. We only collect data that is voluntarily submitted by users when engaging in transportation services, such as parking, micro-mobility and permitting. All data provided by users remains private except for the anonymized or necessary data shared with the client city. Credit card and transaction data is never sold or privatized.
- We won't use personally identifiable information for any purpose other than to support the services authorized by our clients and to deliver and improve Passport products and services. We will not sell personally identifiable information to any third parties under any circumstances.
- We do not share any city data or user transaction data with any third party not directly affiliated with our applications offerings.

We ensure privacy and security

- We comply with all applicable laws and regulations concerning privacy and data protection including the California Consumer Privacy Act (CCPA) and the EU General Data Protection Regulation (GDPR).

- We take all reasonable steps to protect the security of data, utilize reputable third party security testing and intrusion prevention services to audit and validate our efforts, and maintain certifications and/or compliance with all applicable industry payments and data standards including PCI-DSS Level 1 and SSAE-18.

We deliver a digital infrastructure that supports open APIs

- We provide open API access allowing only authorized third party service providers to assist customers in transacting with our clients (for example, a map application from which a motorist can initiate a parking transaction). We believe that our clients benefit from simplified integrations that avoid vendor lock-in and promote user freedom of choice.
- Any authorized third party affiliated with our applications will have access only to the data needed to complete its part of any relevant transactions. Passport's use of such data will continue to be governed by these principles.
- We are committed to the development and integration of commonly accepted data standards that support data portability, simplify integrations, and avoid data-based vendor lock-in. We believe in freedom of choice for our users.

We support client right of use to inform policy and planning

- We provide access to aggregated and anonymized data to our clients for municipal planning, program management, public engagement, and any other municipal purpose to the extent consistent with Passport's Privacy Policy, and support our clients in making data-driven decisions and policies based on our expertise across more than 800 clients of all sizes and mobility environments.
- In connection with this purpose, we work to build bridges with academic or other researchers with appropriate safeguards for privacy.

Search

Search

- Products
- Parking Management Software
- Parking Enforcement Software
- Digital Parking Permits
- Mobility Management

- Our Apps
- Passport Parking

We are HONK MOBILE INC. (**“HonkMobile”, “we” or “us” or “our”**). The following is our Privacy Policy (**“Privacy Policy”**).

This Privacy Policy explains how we collect, use, disclose and safeguard the personal information that you or a third party provide. Providing information or authorizing a third party to disclose personal information to us signifies your consent to our collection, use and disclosure of your personal information in accordance with this Privacy Policy.

1. For the purposes of this Privacy Policy, **“personal information”** means information that can identify an individual directly or through other reasonably available means, including without limitation, name, image (which may be in photos or videos), postal or zip code, motor vehicle information, parking history and credit card information. We will use and disclose your personal information in order to provide our products and services (**collectively, the “Services”**), send you information about the Services and products and services offered by third parties, as well as to make advertising available to you both via our Services and elsewhere.

2. Consent to Terms of Privacy Policy

By providing personal information to us, you are consenting to the collection, use and disclosure of same pursuant to the terms of this Privacy Policy.

The choice to provide us with personal information is always yours. Upon request, we will explain your options of refusing or withdrawing consent to the collection, use and release of your information, and we will record and respect your written choices. However, your decision to withhold particular details may limit the services we are able to offer. **For example, if you do not allow us to collect your credit card information, name and birthdate, we may not be able to offer mobile payment processing.**

3. Electronic Communication

Privacy Officer of HonkMobile at privacy@honkmobile.com. Any questions or concerns with respect to communications from HonkMobile may be addressed to Privacy Officer at privacy@honkmobile.com.

We comply with Canada's Anti-Spam Law, and so we ask each of our users to execute a consent by clicking "I agree" that confirms that we have our user's consent to send commercial electronic messages.

4. Our Privacy Principles

4.1 Identifying Purposes and Obtaining Your Consent

We identify the purposes for collecting your personal information at or before the time it is collected. We will not collect, use or disclose your personal information without your consent, unless required to perform the Services or permitted to do so by law.

At HonkMobile, we collect, use and disclose personal information about you as defined in paragraph 1 of this Privacy Policy. Should we require your information to fulfill a purpose that is not identified in this Privacy Policy, we will obtain your consent before proceeding.

We do not share personal information with companies, organizations and individuals outside of HonkMobile unless we have your consent. We will collect, use and/or disclose your information for the following reasons:

1. **For external processing.** We may provide personal information to our affiliates or other trusted businesses or persons to process it for us, based on our instructions and in compliance with this Privacy Policy and any other appropriate confidentiality and security measures. Your personal information may be stored and processed in Canada, the United States or another jurisdiction and may be subject to the laws of that country or jurisdiction. You expressly consent to such storage and processing.
2. **Service-Related Purposes.**
    1. internal record keeping;
    2. to provide you with Services by processing and fulfilling and/or refund your order;

5. to administer and operate our contests, promotions and programs;
6. to improve our Services and to periodically send you promotional emails about new products, special offers or other information which we think you may find interesting using the email address which you have provided.

3. **For legal reasons.** We will share personal information with companies, organizations or individuals if we have a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to:

1. meet any applicable law, regulation, legal process or enforceable governmental request.
2. enforce applicable terms of service, including investigation of potential violations.
3. detect, prevent, or otherwise address fraud, security or technical issues.
4. protect against harm to the rights, property or safety of HonkMobile, our users or the public as required or permitted by law.

5. Limiting the Collection, Use and Disclosure of Your Personal Information

5.1 The Information We Collect

We collect personal information by fair and lawful means and limit collection to that information which is necessary for the purposes identified in this Privacy Policy and as otherwise required by law. The type of personal information that we may ask for includes:

1. Your name;
2. Mobile telephone number, email address and postal or zip code;
3. Motor vehicle information, including license plate number(s);
4. Credit card or other payment information;
5. Information we obtain from your use of the Services. This information may include:

1. **Device information.** We may collect device-specific information (such as your hardware model, operating system version, unique device identifiers, and mobile network information including phone number).

2. Internet protocol address.
3. device event information such as crashes, system activity, hardware settings, browser type, browser language, the date and time of your request and referral URL.
4. cookies that may uniquely identify your browser or your account.

3. **Location information**. When you use the Services, we may collect and process information about your actual location, like GPS signals sent by a mobile device. We may also use various technologies to determine location, such as sensor data from your device that may, for example, provide information on nearby Wi-Fi access points and cell towers.
4. **Unique application numbers.** This number and information about your installation (for example, the operating system type and application version number) may be sent to HonkMobile when you install or uninstall that service or when that service periodically contacts our servers, such as for automatic updates.
5. **Local storage.** We may collect and store information (including personal information) locally on your device using mechanisms such as browser web storage (including HTML 5) and application data caches.
6. **Cookies and anonymous identifiers.** We use various technologies to collect and store information, and this may include sending one or more cookies or anonymous identifiers to your device.

6. Any other information that we reasonably believe is necessary to allows us to provide the Services.

The choice to provide us with your personal information is always yours. However, your decision to withhold particular information may limit our ability to provide you with the Services.

On occasion, you will be asked to update your consent to ensure that our files remain accurate and in order to comply with our legal obligations. You are encouraged to advise HonkMobile of any changes to your personal information that may be relevant to the services provided to you.

5.2 How Your Information is Collected

believe that a third party has inappropriately disclosed your personal information to us, please contact that third party directly. If the third party does not sufficiently respond to your inquiries, please let us know immediately.

Web cookies are very small text files that are stored on your computer from our Services to keep track of information about your browsing history on our Services. Through the use of web cookies, we may monitor the ads you see and the number of times you view them. The use of cookies also allows us to capture standard web traffic information, such as the time and date you visited our Services, your IP address, and your browser information. In no circumstances do the cookies capture any information that can personally identify you.

5.3 Disclosure to Third Parties

Information you provide may be shared with the merchants or third party service providers with which HonkMobile has entered into a business relationship in order to provide the Services. In addition, HonkMobile may sell, disclose or otherwise use personal information to third parties on an aggregated basis.

We may also disclose your personal information to third parties if required or permitted by law.

We may be legally required to disclose personal information pursuant to government requests, government audits, criminal investigations or government tax reporting requirements. In some instances, such as a legal proceeding or court order, we may also be required to disclose your personal information to authorities. We take precautions to satisfy ourselves that the authorities that are making the disclosure request have legitimate grounds to do so.

Your personal information may be disclosed in situations where we are legally permitted to do so, such as in the course of employing reasonable and legal methods to enforce your or our rights or to investigate suspicion of unlawful activities. We may release certain personal information when we believe that such release is reasonably necessary to protect the rights, property and safety of ourselves and others.

accurate, complete and up-to-date as necessary. If desired, you may verify the accuracy and completeness of your personal information in our records.

Despite our best efforts, errors sometimes do occur. Should you identify any incorrect or out-of-date information in your file, we will remedy any such errors on a timely basis. In the event that inaccurate information is mistakenly sent to a third party, we will communicate relevant changes to the third party where appropriate.

5.5 Data Retention

Your personal information will be deleted if you have not used the Services for thirty-six (36) consecutive months or upon such time as you notify HonkMobile, in writing, that you no longer wish to use the Services.

6. Protecting Your Personal Information

We endeavour to safeguard your information through the employment of reasonable physical, technological, and administrative security measures. However, as you know, no method is 100% secure. Our security practices are reviewed on a regular basis and we strive to use measures that we reasonably believe will keep your personal information safe.

7. Addressing Your Inquiries and Concerns

We are happy to provide you with a copy of this Privacy Policy and to discuss any of its content with you. Upon request, we will also inform you of: the type of personal information we have collected; how your personal information has been used; and any third parties to whom your personal information has been disclosed.

Please direct all questions or enquiries about this Privacy Policy to HonkMobile's Privacy Officer at: privacy@honkmobile.com.

8. Erasure

You have the right to obtain from us the erasure of your Personal Data.

At any time, you may delete your Account and uninstall the App. Deleting your account can be accessed in your account settings page.

delete some of your Personal Data to the extent that it is still required for discharging our legal obligations. We may also retain, use, and share your Anonymized Data that we previously collected prior to your deletion of your Account.

9. Updating this Privacy Policy

Any changes to our privacy standards and information handling practices will be reflected in this Privacy Policy in a timely manner. HonkMobile reserves the right to change, modify, add, or remove portions of this Privacy Policy at any time. Please check our Services periodically for any modifications. To determine when this Privacy Policy was last updated, please refer to the modification date at the bottom of this Privacy Policy.

10. Services Governed by this Privacy Policy

Our Services are governed by the provisions and practices stated in this Privacy Policy. Our Services may contain links to third party sites that are not governed by this Privacy Policy. Although we endeavour to only link to sites that share our commitment to your privacy, please be aware that this Privacy Policy will no longer apply once you leave our Services and that we are not responsible for the privacy practices of third party sites. We therefore suggest that you closely examine the respective privacy policies of third party websites to learn how they collect, use and disclose your personal information.

11. Governing Law

This Privacy Policy and all related matters are governed solely by the laws of the Province of Ontario and the applicable Federal laws of Canada.

12. Personal Information Outside of Canada

HonkMobile may perform activities outside of Canada through third parties. You acknowledge and agree that, as a result, your personal information may be processed, used, stored or accessed in other countries and may be subject to the laws of those countries. For example, information may be disclosed in response to valid demands or requests from government authorities, courts, or law enforcement in other countries.

About
Our Products
The Future of Payment

Contact
Press
Blog

Privacy Policy
Terms & Conditions
Refund Policy

About
Our Products
The Future of Payment

Contact
Press
Blog

Privacy Policy

Choose Your Language

Thank you for using ParkMobile!

At ParkMobile, we are committed to respecting your privacy. This policy i
you understand how we collect, use, and share information that we colle
ParkMobile websites, mobile applications, and other services we operat
internet company, some of the concepts below are a little technical and c
but we've tried our best to explain things simply and transparently. If you h
about our privacy policy, please **let us know**.

What's changed

- We updated our toll-free number;
- We made it easier for you to update your **cookie preferences**;
- We added more details about the data we collect and how it's used;
- We made some stylistic changes so that our policy is easier to read

What information we collect

You may be asked to provide personal information anytime you interact v
affiliates, such as when you use one of our mobile apps. The types of info
depends on how you use our services. We collect information in a few dif

1. When you give it to us or give us permission to obtain it

When you sign up for or use ParkMobile you voluntarily share certain infc
your name, telephone number, email address, payment card information,
information, and any other information you give us. When you use ParkM
parking transaction, we collect information related to the transaction, suc

2. When a third-party gives it to us

We may collect your information when a third-party provides your inform our services. For example, your friend may provide us with your license p pays to park your car using her ParkMobile account. If your employer has account with ParkMobile, your employer may provide us information nec your account.

3. We collect technical information when you use our Services

When you use a website, mobile application or other internet service, cer electronic network activity information gets created and logged automat true when you use ParkMobile. Here are some of the types of informatior

- **Internet or other electronic network activity information,** such about your interactions with our Services. This includes informatior content you view, the time you spend viewing the content, and the f access on the Services that we collect using cookies, pixels, and ot technologies;
- **Identifiers,** such as your Internet Protocol (IP) address, device ider (including the manufacturer and model), and Media Access Contro address;
- **Geolocation data,** such as where you are located when you use ou
- **Standard server log data,** such as your application version numbe type (Windows or Macintosh), screen resolution, operating system and version, and the date and time of your visit.

We may also aggregate or de-identify the information described above. A identified data is not subject to this policy.

How we use your information

We collect and use your information so that we can operate effectively ar the best experience when you use our app and/or web products. We alsc information we collect for the following purposes:

- **Fulfillment of parking transactions and other purchases,** such a your parking transaction; supplying the purchased services; and cc

and addressing concerns raised by you; and monitoring and improv customer support responses;

- **Improving our services**, such as conducting data analysis and auc new products and services; enhancing our websites and mobile ap our services; identifying usage trends and visiting patterns; conduc satisfaction, market research, and quality assurance surveys; deter effectiveness of our promotions; meeting contractual obligations;
- **Marketing and promotions,** such as sending you emails and mess news and new promotions, features, products and services, and co you with relevant advertising on and off our services; and administe participation in contests, sweepstakes and promotions; and
- **Legal proceedings and requirements,** such as investigating or ac claims or disputes relating to your use of our services; or as otherwi applicable law; or as requested by regulators, government entities, inquiries.

How and when we share your information

We may share the information we collect with:

1. Our wholly-owned subsidiaries and affiliates

We share information within the ParkMobile family of companies that hel services or conduct data processing on our behalf. If we were to engage acquisition, bankruptcy, dissolution, reorganization, or similar transactior involves the transfer of the information described in this policy, we would information with a party involved in such a process (for example, a potent

2. Third-party companies, service providers or business partners

We rely on third parties to perform a few contractual services on our beh may need to share your information with them. For example, we may rely providers to enable functionality on our Services, to provide you with rele (including advertisements), to process your payments, and for other bus

3. Municipalities and private parking operators

We share your information with our municipality and other business partı have a contractual agreement in order to provide services to you. For exa will have access to your vehicle information for parking enforcement pur

4. Parking enforcement companies

Our clients frequently contract with third-party companies to enforce pa
and their parking facilities. We may share your license plate number with
enforcement companies to confirm that you have paid to park at the facil

5. Law enforcement agencies or government agencies

We may share information with law enforcement agencies and/or the juc
confirm or dispute a traffic citation issued to you. We may also disclose in
believe that disclosure is reasonably necessary to comply with a law, reg
request; to protect the safety, rights, or property of the public, any persor
to detect, prevent, or otherwise address fraud, security or technical issue

6. Your consent

We may share your information other than as described in this policy if w
you agree.

7. Other services

We may share your information with third parties to enable you to sign up
ParkMobile, or when you decide to link your ParkMobile account to those

Where we store your information

We process and store personal information inside and outside of the Uni
including in countries that have privacy protections that may be less strin
jurisdiction.

How we secure your information

Although we take steps to safeguard personal information, no practices
and we do not guarantee the security of your information.

How we use cookies

We, along with our partners, use various technologies to collect and stor
you visit one of our services, and this may include using cookies or simila

Ready to Park
Reserve Parki
Solutions for P
More +
Blog
Contact Us
Fleet Sign In

The technologies we use for this automatic data collection may include:

- **Cookies.** A cookie is a small file placed on the hard drive of your co cookies to store information, such as your login credentials and wel preferences, so that we can remember certain choices you've mad also be used to recognize your device so that you do not have to pr information more than once.
- **Web beacons.** Pages of our services or our e-mails may contain sr files known as web beacons (also referred to as clear gifs, pixel tags pixel gifs) that permit us, for example, to count users who have visite or opened an e-mail and for other related website statistics (for exa the popularity of certain website content and verifying system and
- **Mobile device identifiers and SDKs.** A mobile SDK is the mobile a web beacon. The SDK is a bit of computer code that app developer their apps to enable ads to be shown, data to be collected, and relat analytics to be performed.
- **Other technologies.** There are other local storage and Internet tec such as local shared objects (also referred to as "Flash cookies") ar storage, that operate similarly to the technologies discussed above

You may be able to refuse or disable cookies by adjusting your web brow browsers have options that allow the visitor to control whether the brows cookies, reject cookies, or notify the visitor each time a cookie is sent. Be browser is different, please consult the instructions provided by your wel in the "help" section). Please note that you may need to take additional st disable local shared objects and similar technologies. For example, local be controlled through the instructions on Adobe's **Setting Manager** pag refuse, disable, or delete these technologies, some of the functionality of no longer be available to you, and any differences in service are related to cookies may, in some cases, cancel the opt-out selection in your browse

Some of our third-party partners are members of the Network Advertisir offers a single location to opt-out of ad targeting from member companie please click **here** or **here**. For additional information on how Google proc information and what choices you may have, visit their site **here**. Due to d websites and mobile apps, you may need to take additional steps to opt- based advertising for mobile applications. Please check your device sett

Ready to Park

Reserve Parki

Solutions for F

More +

Blog

Contact Us

Fleet Sign In

cookie preferences for our website any time.

Do not track signals and similar mechanisms. Our website is not conf respond to "do not track" settings or signals in your browser headings.

Your choices and rights

You have options relating to the information that we have about you. You options, by completing our **privacy request form**.

- **Promotional emails and other marketing material.** You can unsu receiving marketing material from us at any time by clicking the unsu located at the bottom of our emails or by emailing us at **privacy@pa** Unsubscribing from promotional material will not prevent you from r transactional, relationship, or non-commercial content from us.
- **Cookies and third-party advertising.** You can update your **cooki** for our website any time. For instructions on how to adjust cookie se out of third-party ad targeting in general, click **here**.

Depending on where you live, you may have certain additional rights to:

- Request access to your personal information; and
- Request deletion of your personal information

Your California Privacy Rights. If you are a California resident, you may information regarding the disclosure of your personal information to third direct marketing purposes. To make such a request, please send an ema **privacy@parkmobile.io** or write us at Parkmobile, LLC, Attn: Privacy De Spring Street, NW, Suite 200, Atlanta GA 30309.

California residents

The California Consumer Privacy Act (CCPA) requires us to disclose cat information we collect and how we use it, the categories of sources from personal information, and the third parties with whom we share it, which above.

We are also required to communicate information about rights California under California law. California residents may exercise the following right

- **Right to delete.** You may submit a verifiable request to close your a will delete personal information about you that we have collected;
- **Right to know and access.** You may submit a verifiable request for regarding: (1) categories of personal information we have collected of sources from which we collect personal information; (3) our busi commercial purpose for collecting personal information; (4) categc parties with whom we share personal information; and (5) specific p personal information it has collected about you.
- **Right to opt out.** You may submit a verifiable request that we not "s by CCPA) your personal information to third parties.
- **Right to equal service.** We will not discriminate against you for exe privacy rights.

Just to clarify - we do **not** sell your personal information to any third party monetary consideration. However, like most companies, we do share info be considered a "sale," as defined by the CCPA. This includes sharing ide commercial information and internet or other electronic network activity networks and website analytics companies. You can always opt out of th

updating your cookie preferences.

If you would like to exercise your rights, please contact us via one of the f

- **Complete our online form**
- **Call us** toll-free at **(877) 727-5457**
- **Email us** at **privacy@parkmobile.io**
- **Write to us** at Parkmobile, LLC, Attn: Privacy Department, 1100 Spr Suite 200, Atlanta, GA 30309

To complete your request, you may be asked to provide additional inform identity, such as the license plate number and/or last four digits of a credi with your account. We will compare the information you provide to any in

Ready to Park

Reserve Parki

Solutions for P

More +

Blog

Contact Us

Fleet Sign In

receive it. The information collected through this process will be used for purposes only.

If you would like to use an agent registered with the California Secretary of your rights, we may request evidence that you have provided such agent attorney or that the agent otherwise has valid written authority to submit exercise rights on your behalf.

Children's data

Children under 16 are not allowed to use our services. If we learn we have received personal information from a child under 16 without verification of we will delete that information. If you believe we might have any informati child under 16, please contact us at **legal@parkmobile.io**.

How we make changes to this policy

We may change this policy from time to time, and if we do, we'll post any c page. If you continue to use ParkMobile after those changes are in effect new policy. If the changes are significant, we may provide a more prominent your consent, as required by law.

Contact us

Questions, comments, and complaints about ParkMobile's data practice chief privacy officer by sending an email to **privacy@parkmobile.io** or w Parkmobile, LLC, Attn: Privacy Department, 1100 Spring Street, NW, Suite 30309. You can also call us toll-free at **(877) 727-5457**.

Last Updated

Our privacy policy was last updated on July 31, 2020.

Ready to Park
Reserve Parki
Solutions for P
More +
Blog
Contact Us
Fleet Sign In

PayByPhone is committed to respecting your privacy and complying with all applicable data protection and privacy laws. In this Privacy Policy, we describe how we collect, use, share and protect your Personal Data.

As part of our commitment to you, we ensure that your Personal Data is accurate, confidential, and secure and allow you to access, correct, or erase your Personal Data. Please note that in order to offer our Services, we transfer your Personal Data to Canada and to certain service providers which may be located in other countries.

When you create an Account with us or use our Services, you agree to this Privacy Policy and the Terms and Conditions. Each time you use your Account or our Services, or provide us with information, the current version of this Privacy Policy and the Terms and Conditions govern the processing of your Personal Data.

If you do not agree with the terms of this Privacy Policy or the Terms and Conditions, please refrain from creating an Account or using our Services.

If you have any questions or comments about this Privacy Policy, please contact the relevant Data Protection Officer at the address listed in Section 15 below.

SPECIAL NOTICE REGARDING CHILDREN

Our Services are not directed to people under 16. We do not knowingly collect personal information from children under 16. If you become aware that a child has provided us with Personal Data without the proper consent, please contact the relevant Data Protection Officer at the address listed in Section 15 below and we will take steps to remove such information and terminate the account, as necessary.

Table of Contents

1. Who processes your information?

Your contract and Account may be with PayByPhone Technologies Inc. or one of its subsidiaries, including without limitation PayByPhone US Inc. (United States), PayByPhone Limited (United Kingdom), PayByPhone SAS (France, Monaco, Netherlands, Belgium), PayByPhone Suisse AG (Switzerland), PayByPhone Italia S.r.l. (Italy) or sunhill technologies GmbH (Germany). Collectively, all of these entities are referred to here as "PayByPhone". The applicable contract party depends on the country from which you open your Account and in which you conduct your Parking Sessions, as set out in the Terms and Conditions in greater detail.

Your PayByPhone contract party and PayByPhone Technologies Inc., incorporated in Canada, are jointly responsible for the processing of your Personal Data, including in the context of the registration for and general use of the Services, product and system development including ensuring IT security, and for advertising and marketing purposes. The controllers have agreed among themselves who will fulfill specific obligations with respect to the data processing and shall work closely together. In particular, they will provide each other with the information necessary to fulfill their respective obligations and to enable the exercise of data subject rights.

You will have statutory protection in the applicable territories and this Privacy Policy is without prejudice to those statutory rights.

PayByPhone is committed to complying with all applicable privacy laws ("Data Protection Laws"), including without limitation the Canadian Personal Information Protection and Electronic Documents Act ("PIPEDA"), the European General Data Protection Regulation ("GDPR") and the UK General Data Protection Regulation ("UK GDPR").

Facilities Operators for the locations where you park process parts of your Personal Data which relate to the Parking Sessions at their parking facilities and which, among other things, enable them to effect parking validation, enforcement and fines.

For information on additional processors of your Personal Data, see section 5 below.

2. What information is processed?

We only collect and process Personal Data that is required to create an Account and to offer the Services you request and to communicate with you.

You and anyone you authorize to use your Account provide some of this information directly when you create an Account, use a Service or contact us for support, including:

- Mobile phone number
- Vehicle license plate
- Billing information (such as credit card and debit card numbers and expiry dates) (NOTE: We do not store CVV/CVV2 security numbers on our servers.)
- Password
- Transaction data (such as Parking Session date, time, duration, zone number and amount paid)
- Customer support issue details
- Email address

In some cases, for example when you permit another party, such as your employer, to pay for parking sessions on your Account through linking your Account to theirs and adding their payment method to your Account, we ask you or the owner of the payment method to provide your:

- Profession
- Professional affiliations membership
- Work email address
- Unique username

- Work mobile phone number
- Job Title
- Department
- Office Name
- Employee Cost centre

You may also give us additional information when you choose to open your Account using information from third party services you already have, including:

- Your device settings and credentials
- Credentials from a third-party app or platform

You may also choose to give us additional information to obtain a Service or receive communications from us including:

- Name
- Postal code/zip code
- Location
- Type of vehicle
- Communication preferences
- Any information related to your voluntary participation in our contests, promotions, and research, including demographic or occupation information that you choose to provide

You may stop providing us this additional information at any time by adjusting your Account settings in the App, on the Site or by contacting us.

We also collect other data indirectly when our software interacts with your device and when we use technologies like cookies and error messages. This may include:

- IP address and information about the device you use to access the Services
- Media Access Control (MAC) address
- Operating system name and version
- Device manufacturer and model
- Your language preferences
- Type and version of your Internet browser
- Name and version of the App you use
- Site traffic data
- Landing and exit page details
- Details of your session between pages of the Site to provide a continuity of experience
- Details of when you install and uninstall the App

Please see our Cookies Policy for more information.

We also sometimes obtain data about you from third parties (including parking operators, payment facilitators, parking enforcement agencies and hardware/software manufacturers). For example:

- When you register a credit card or debit card with us to use the Service, we will use card authorization and fraud screening services to verify that your card information matches other information that you supply to us, and that the card has not been reported as lost or stolen.
- When you opt into Autopass (available in some countries), a Service that allows you to automatically pay for parking at facilities that support automatic number plate recognition, we will obtain from the parking operator the time of the vehicle entry and exit from the parking facility and we may receive a photograph of the vehicle taken at that time.

3. Why is your information processed?

We process your information so that we can offer you our Services and communicate with you.

Contractual Relationship

When we process your Personal Data in relation to our Services (including, without limitation, for customer service, security messages, processing payments, sending receipts and reminders of parking session expiry) and our related internal purposes (including administration, risk management, compliance, product development, research, debt collection, financial audit, security and record keeping,) we rely on the lawful basis of having a contractual relationship with you.

Consent

When we process your information to communicate with you (including about our and our affiliate promotions, events occurring in localities where you recently parked, targeted advertising and marketing of services), we rely on the lawful basis of consent to process your Personal Data and we are committed to obtaining that consent in a legitimate way.

You can provide your consent in the App, on the Site or verbally to our authorized representatives. You will be asked specifically if you would like to opt-in to each of these communications and you can choose whether to receive some, all, or none of these communications.

Unless the type of use is necessary for us to provide the Services, you will have the right to remove your consent to such use at any time (more on this below) by logging in to your Account on the Site, in the App or by calling your Customer Support Center or writing to your respective Data Protection Officer at the contact listed in Section 15 of this Privacy Policy. You will have an opportunity to unsubscribe each time we communicate with you. Note that your decision to withhold or withdraw your consent to certain other uses of Personal Data or certain types of communication may restrict our ability to provide a particular service or product.

Subject to Data Protection Laws, we may collect, use, store or share Personal Data without your consent in the following limited circumstances:

- As instructed by local authorities in emergency situations that threaten an individual's life, health, or personal security such as emergency warnings for tsunami or earthquakes.
- When the Personal Data is available from a public source (e.g. a telephone directory).
- To protect ourselves and other users from fraud.
- To investigate an anticipated breach of an agreement or a contravention of law.
- When such collection, use or disclosure of Personal Data is permitted or required by law.

Legitimate Interest

Where permitted by law, we will process your Personal Data on the basis of our legitimate interest, for example when contacting you about new product offerings and conducting customer satisfaction surveys to enhance our services or sending you newsletters and parking, vehicle or road use related service and security messages. For this type of processing, we will always take into consideration the effect of such processing on your fundamental rights and freedoms, and if we believe that the communication would be an infringement on your rights, we will not proceed with that communication.

PayByPhone Technologies Inc. acts on the basis of legitimate interest in the group-wide use of a central IT infrastructure (including for registration and processing of parking transactions, product and system development and ensuring IT security).

You may opt-out of receiving legitimate interest-based communications by logging in to your Account on the Site or in the App or by calling your Customer Support Center or writing to your respective Data Protection Officer at the contact listed in Section 15 of this Privacy Policy. Note that your decision to opt-out may restrict our ability to provide a particular service or product.

4. How is your information processed?

We only process your Personal Data for the purposes for which we have a lawful basis.

Some processing associated with the purpose of providing you our Services include:

- Creating your Account.
- Operating the Service.
- Providing you with navigation services to your parking location.
- Providing you with parking information at or near you or at your location.
- Sending you notifications of the end of your parking session.
- Facilitating, processing, and keeping a record of your Transactions.
- Serving as the merchant of record for certain Transactions.
- Collecting or attempting to collect any unpaid amounts owed by you.
- Sending you the receipt for your Transactions.
- Providing you with your parking history.
- Facilitating communication between you and PayByPhone.
- Providing you customer support.

- Cooperating with relevant authorities (for example: regarding your Parking Penalties).
- Analyzing and monitoring App and Service usage and making improvements, enhancements, and customizations to your experience.
- Investigating and resolving outages, malfunctions, or problems that you may be having with our App or Services.
- Ensuring the security of the App and Services, preventing fraud, and enforcing our policies.
- Complying with any applicable law and assisting law enforcement agencies under applicable law.
- Working with you to terminate your Account and retaining only your Personal Data when we are required to retain such information by law or pursuant to our other agreements.
- Responding to any dispute, or legal proceeding of any kind between you and PayByPhone.
- Providing required reports to our financial partners or service providers.
- Creating Anonymized Data sets for internal, external, commercial, and analytical purposes.
- Performing other activities with your consent.

Some processing associated with the purpose of communicating with you include:

- Sending you updates, notices, announcements, and additional information related to our Services, vehicle, parking or road use related service and security messages, or information about events occurring in localities where you recently parked.
- Conducting surveys, contests, questionnaires, discounts or rewards programs, sweepstakes, or promotions for ourselves.
- Sending you marketing, advertising material, and other content and provide you with information and advertisements about offers, discounts and other services relevant to you, or that we believe you may find interesting.
- Sending you updates, notices, announcements, and additional information related to other products and services or those of our affiliates or those of other third parties.
- Conducting surveys, contests, questionnaires, discounts or rewards programs, sweepstakes, or promotions on behalf of our affiliates or third parties.

5. With whom is your information shared?

We will never use or disclose your Personal Data unless we have a lawful basis to do so.

We do not sell your Personal Data to parties outside of PayByPhone. We will not rent, license or exchange customer lists or your Personal Data to other parties outside of PayByPhone, except as we describe below.

No Personal Data will be shared with third parties, except as required to offer the Services to you or as you specifically consent. We may:

- Send your vehicle information to parking operators and parking enforcement agencies to confirm your parking sessions.
- Send some information to third party service providers that help us to operate our Services including, but not limited to, website hosting, data warehousing, data analysis, event logging, information technology, customer service, user analytics, email delivery, messaging, auditing, and debt collecting.
- Send your credit or debit card payments to our payment processors.
- Send some information to police, security forces, competent governmental, intergovernmental or supranational bodies, competent agencies, departments or regulatory, self-regulatory authorities or organizations or other third parties where the information is subject to disclosure in accordance with the applicable law, or where we believe, in good faith, it is appropriate to cooperate with in relation to investigations of fraud or other illegal activity or potential illegal activity, or to conduct investigations of violations of our Terms and Conditions.
- Send some information to auditors in connection with independent audits of our financial statements and operations. These auditors cannot use personally identifiable information for any secondary purposes.
- Share your Personal Data with a potential purchaser of PayByPhone (or the majority of its assets), or a merger, reorganization, or internal acquisition.
- Send information to our affiliates, including for example members of the Volkswagen Group, as allowed by law. Any Personal Data relating to you that we provide to our affiliates will be treated by those affiliates in accordance with this Policy and we are responsible for the management of the jointly used Personal Data.
- Disclose aggregated statistical data for statistical or public relations purposes. For example, we may disclose that a specific percentage of our users drive a blue car. However, this aggregated information is not tied to personal information.
- Share some Anonymized Data with third party partners who use the Anonymized Data to create mobility-related analytics including for example, parking analytics & predictive occupancy as well as parking availability reports.

- Share information with the party which pays for Parking Sessions on your Account through linking your Account, with your permission, to theirs and adding their payment method to your Account. The information shared includes data collected from you, data collected on parking and other transactions including financial information, data collected on your mobile devices, and derivative data used and stored in PayByPhone databases, to the extent that such data relates to the use of third-party payment method added to your Account. The data will be shared primarily for the purposes of verifying parking transactions paid for with the third-party payment methods and generating parking activity reports for the third party.

6. Where is your information transferred?

We will transfer your Personal Data to PayByPhone in Canada, irrespective of the country in which you reside or from which you provide Personal Data.

The transfer of your Personal Data is done in a secure way and in compliance with Data Protection Laws. The European Commission has found, on the basis of Article 45 of the GDPR, that Canada, while not bound by the GDPR, ensures an adequate level of protection of personal data. This adequacy decision took into account Canada's domestic law, its supervisory authorities and international commitments it has entered into.

We may also transfer your Personal Data to third party suppliers in other countries to provide part of our Service to you. In our agreements with these parties, we require them to protect your Personal Data and to adhere to Data Protection Laws and we make sure that they have provided appropriate safeguards.

Your personal information may be accessible to regulatory, law enforcement and national security authorities of those jurisdictions, and may be subject to disclosure in accordance with the laws of those countries.

7. How is your information kept safe?

We have put appropriate technical and organizational protection measures in place to protect your Personal Data from unauthorized access, collection, use, disclosure, copying, modification, disposal or similar risks.

PayByPhone commits to the following security measures:

- All Personal Data of users is stored electronically on an encrypted database of PayByPhone protected by a firewall.
- The PayByPhone Service is hosted in a secure server environment that uses a firewall and other advanced technology to prevent interference or outside access.
- Physical access to the database where Personal Data is stored and the servers where the PayByPhone Service is hosted is protected by 24/7 guards who only allow authorized personnel access to the database, such personnel is limited to those that need access.
- PayByPhone complies with PCI Data Security Standard Level-1 with a robust security process for payment card data and other Personal Data, including prevention, detection and appropriate reaction to security incidents.
- Parking transactions processed through our Services are encrypted using x-bit (for example 128-bit) secure sockets layer (SSL).
- PayByPhone uses appropriate security measures when destroying customers’ Personal Data such as deleting electronically stored information.

We will continually review and update our security policies and controls as technology changes to ensure the ongoing security of your Personal Data.

8. How long is your information retained?

PayByPhone will retain your data in accordance with Data Protection Laws.

We will retain your Personal Data (including information related to each parking session and to each of your Transactions) for only so long as is reasonably necessary to fulfil the purposes for which the information was collected or as required by law.

If you create an Account with us, we will retain your Personal Data as long as you have that Account. If you close your Account or if there is no activity on your Account (including no log-ins and no parking sessions) for a period of more than 3 years, we will mark your Account in our database as "Closed," but may have to keep some information for as long as is required to comply with our legal obligations or 7 years, whichever is shortest.

9. What rights do you have with regards to your information?

According to the controller arrangement between your PayByPhone contract party and PayByPhone Technologies Inc., your PayByPhone contract party is responsible for fulfilling the obligations related to data subject rights.

You can contact the relevant local Data Protection Officer at the address set out at Section 15 below with requests related to the rights described below. You are also free to assert your data subject rights against PayByPhone Technologies Inc. at the contact listed in the first line of Section 15 below.

Any request must be made to PayByPhone in writing and provide sufficient detail to identify the Personal Data that it relates to. PayByPhone may request that you verify your identity. PayByPhone will address the request within 30 business days or provide written notice of an extension where additional time is required to fulfil the request.

Access

You have the right to request access to your Personal Data, to know how we use it and to whom we have disclosed it, subject to certain limited exceptions.

You can assert this right by accessing your Account on the Site or the App. You may also contact us with a Personal Data access request and we will take all reasonable steps to assist you with any legitimate request for access.

We may not be in a position to respond to a data access request. If a request is refused in full or in part, we will notify you in writing and provide the reasons for refusal and the recourse available to you.

Rectification

You have the right to make sure that your Personal Data is accurate.

We make reasonable efforts to ensure that all of our users' Personal Data is kept accurate and complete. If you are the Account holder, we provide you with tools to access or modify the Personal Data associated with your Account. You may also request that we correct your Personal Data.

If your Personal Data is demonstrated to be inaccurate or incomplete, we will, so far as practicable and as soon as practicable, correct your Personal Data and send the corrected information to any organization to which we disclosed the Personal Data in the previous year. If the correction is not made, we will note your correction request in your file.

Erasure

You have the right to obtain from us the erasure of your Personal Data.

At any time, you may close your Account and uninstall the App. You may also request that we erase your Personal Data.

In the event that you delete your Account and the App or request erasure of your Personal Data, we will use commercially reasonable efforts to remove your Personal Data from our files, however, we may not be able to delete some of your Personal Data to the extent that it is still required for discharging our legal obligations. We may also retain, use, and share your Anonymized Data that we previously collected prior to your deletion of your Account.

Withdraw consent (when processing is based on consent)

As mentioned above, when PayByPhone is relying on consent as the lawful basis for processing your Personal Data, you may remove such consent at any time, examples of this include:

- For certain types of communications, you can change your preferences in your Account permissions via the settings in the App.
- For emails, you may click on the "Unsubscribe" link in the received email.
- For push notifications, you can change the setting on your mobile device or adjust your Account settings.
- For Cookies on the Site, you can change the Cookies settings on your browser.
- For collection of location information, you can change your location access to our App using your mobile device settings and by adjusting your Account settings.

Please note that changing your consent may result in a change in your Services and experience.

Lodge a complaint

You have the right to communicate with PayByPhone about any issues that you may have relating to your Personal Data.

The Data Protection Officer of your respective PayByPhone contract party is responsible for ensuring PayByPhone's compliance with this Privacy Policy and Data Protection Laws. You should direct any complaints, concerns or questions regarding PayByPhone compliance in writing to the respective Data Protection Officer at the contact information below in Section 15.

You may also write to the Privacy Commissioner of Canada or the privacy supervisory authority in your country.

10. Definitions

- **Account** - The PayByPhone parking service account opened by you in the App, on the Site or by calling our Customer Support Centers.
- **Anonymized Data** - Anonymous, statistical, or aggregated information, on a de-identified basis (such as anonymous location information, enrollment numbers, demographic group information, etc.), in a form that does not enable the identification of a specific user.
- **ANPR** – The automatic number plate recognition feature which (1) identifies an opted-in vehicle, prior to payment, as authorized to park at the participating parking facilities and allows access to the parking facilities without having to perform any action normally required to remove a barrier to entry and (2) automatically records the time of entry and exit from the participating parking facility, calculates the length of stay and the cost of the Parking Session for the purposes of initiating payment.
- **App** - The PayByPhone mobile parking payment application and other applications that we may develop.
- **Autopass** – The service from PayByPhone that you opt your vehicle or vehicles in using the App, the Site or our Customer Support Center which allows you to automatically pay for parking at participating parking facility operators that support ANPR.
- **Cookies** - The small data files on your computer or other device which consist of cookies, pixel tags, e-tags, "flash cookies", or other local storage provided by your browser or associated applications.
- **Data Protection Officer** - The individual designated as responsible for ensuring that PayByPhone complies with this Privacy Policy and applicable privacy laws, and is listed in the Contacts section below.
- **Facilities Operator** - The operator of a parking facility offering the option to pay for parking with the PayByPhone service.
- **Parking Penalties** - Parking fines, violation notices, tickets, citations, or penalties; your vehicle being wheel booted, your car being towed, or impounded; and other enforcement of vehicle parking requirements.
- **Parking Session** - The parking service you obtain from a Facilities Operator within the Transaction. Details of a parking session can include location, license plate, start parking session time, end parking session time and are usually linked to a payment.
- **Payment Information** - Information of any type necessary to process payments by credit cards, debit cards, digital wallets, in-app and web purchases and any other payment method accepted by PayByPhone now or in the future in connection with any Transaction.
- **Personal Data** - Information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier. Note that not all personal information that is shared with PayByPhone is considered Personal Data.
- **Services** - All services offered by PayByPhone, including those that allow you to pay for a Parking Session at participating parking clients, including Autopass, pursuant to the Terms and Conditions, by using our App, Sites, Application Programming Interfaces, backend technologies, products, services, content, features, functions, applications, IVR System, PayByPhone Portal, PayByPhone Business Portal, and any future updates, changes or additions thereto.
- **Site** - All PayByPhone operated websites including https://www.paybyphone.com, https://www.paybyphone.fr, https://www.paybyphone.co.uk, https://www.paybyphone.ch, https://paybyphone-parken.de, https://www.pbp.it/, as well as any successors to such sites.
- **Terms and Conditions** – Our Terms and Conditions which are accepted and agreed to by you when you open an Account or use the Services and which govern your use of the App and Services.
- **Transactions** – Any time you start, pay for, complete, or make a parking session transaction using our App or Services.

11. App store; links to other websites

Your app store (e.g., iTunes or Google Play) may collect certain information in connection with your use of the App, such as Personal Data, Payment Information, geolocational information, and other usage-based data. We have no control over the collection of such information by a third-party app store, and any such collection or use will be subject to that third party's applicable privacy policies.

Some pages on the Site and the App include links to third party websites. These third-party sites are governed by their own privacy statements, and we are not responsible for their operations, including but not limited to, their information practices. You should review the privacy statement of those third-party sites before providing them with any personally identifiable information. PayByPhone is not responsible for the processing of Personal Data on those third-party sites. We strongly advise you not to share any personal information about your Account, including your account number or password, on any social media site or with any third-party application that is not operated by PayByPhone.

12. Applicable law

All matters related to this Privacy Policy shall be governed in all respects by the laws of and all disputes shall be subject to the exclusive jurisdiction of the competent courts located in the jurisdiction in which the PayByPhone entity with whom you have a contract is domiciled, excluding the application of any conflict of laws principles and/or rules. In the case of PayByPhone Technologies Inc., the relevant jurisdiction is the Province of British Columbia, Canada (subject to the provisions of the Consumer Protection Act applicable to residents of Quebec), in case of PayByPhone US Inc. – the State of Delaware, United States, in the case of PayByPhone Limited - United Kingdom, in the case of PayByPhone SAS - France, in the case of PayByPhone Suisse AG - Switzerland, in case of PayByPhone Italia S.r.l. - Italy and in the case of sunhill technologies GmbH - Germany. Notwithstanding the above, you agree that it shall be nevertheless permissible for PayByPhone to apply for equitable relief in any jurisdiction. You also agree to comply with all local laws, rules, and regulations, including but not limited to those applicable to online conduct and acceptable Internet content.

13. Changes to this policy

We may amend, update, modify, replace, or revise this Privacy Policy at any time by communicating those updates with you and by posting such on our Site. All such amendments, updates, modifications, replacements, versions, or revisions are effective immediately upon posting on our Site. All references in this Privacy Policy to the Terms and Conditions, Legal Notice, and any other Services matters are references to the same as they are amended, updated, modified, replaced, or revised.

14. Further questions

If at any time you would like to contact us with your views about our privacy practices, or with any enquiry relating to your personal information, you can do so by emailing us at the addresses listed below.

15. Contacts

Contact information for PayByPhone Data Protection Officer:

Location	Address	Email
USA and Canada	Suite 403 1168 Hamilton Street Vancouver, BC V6B 2S2 Canada	dpo@paybyphone.com
UK	Bishops Court 17A The Broadway Old Hatfield AL9 5HZ	dpo-uk@paybyphone.com
France, Monaco, Netherlands, Belgium	62bis Avenue André Morizet 92100 Boulogne-Billancourt	dpo-france@paybyphone.com

and Switzerland		
Italy	Via Canton, 11 37055 Ranco all'Adige	dpo-italia@paybyphone.com
Germany	Allee am Röthelheimpark 15 91052 Erlangen	dpo-germany@paybyphone.com

PayByPhone is owned by Volkswagen Finance Overseas B.V.

Last updated: 2021-12-15

paybyphone

PayByPhone is owned by Volkswagen Financial Services AG

Change region

Support and contact

- Help Center
- Contact
- Send us feedback
- Cookies settings

Follow us

-
-
-

About PayByPhone

- About us
- Code of Conduct
- Community Blog
- Contact us

- Leadership Team
- Careers
- DEI at PayByPhone

Get the app

- Map
- Parking operators
- Terms & Conditions
- Privacy
- Whistleblowing

North America

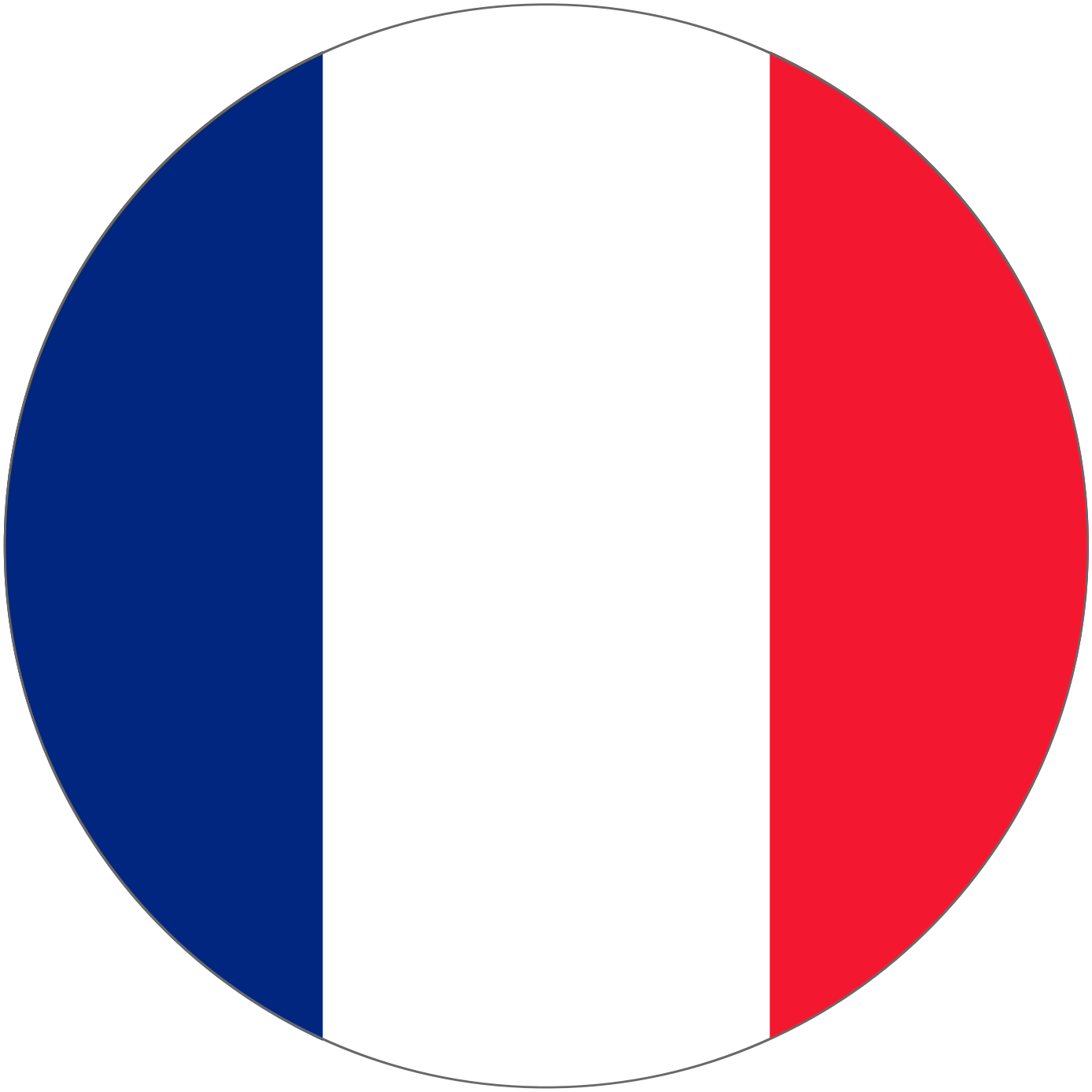
Select your region

- United States

- Canada (EN)

- Canada (FR)

- United Kingdom



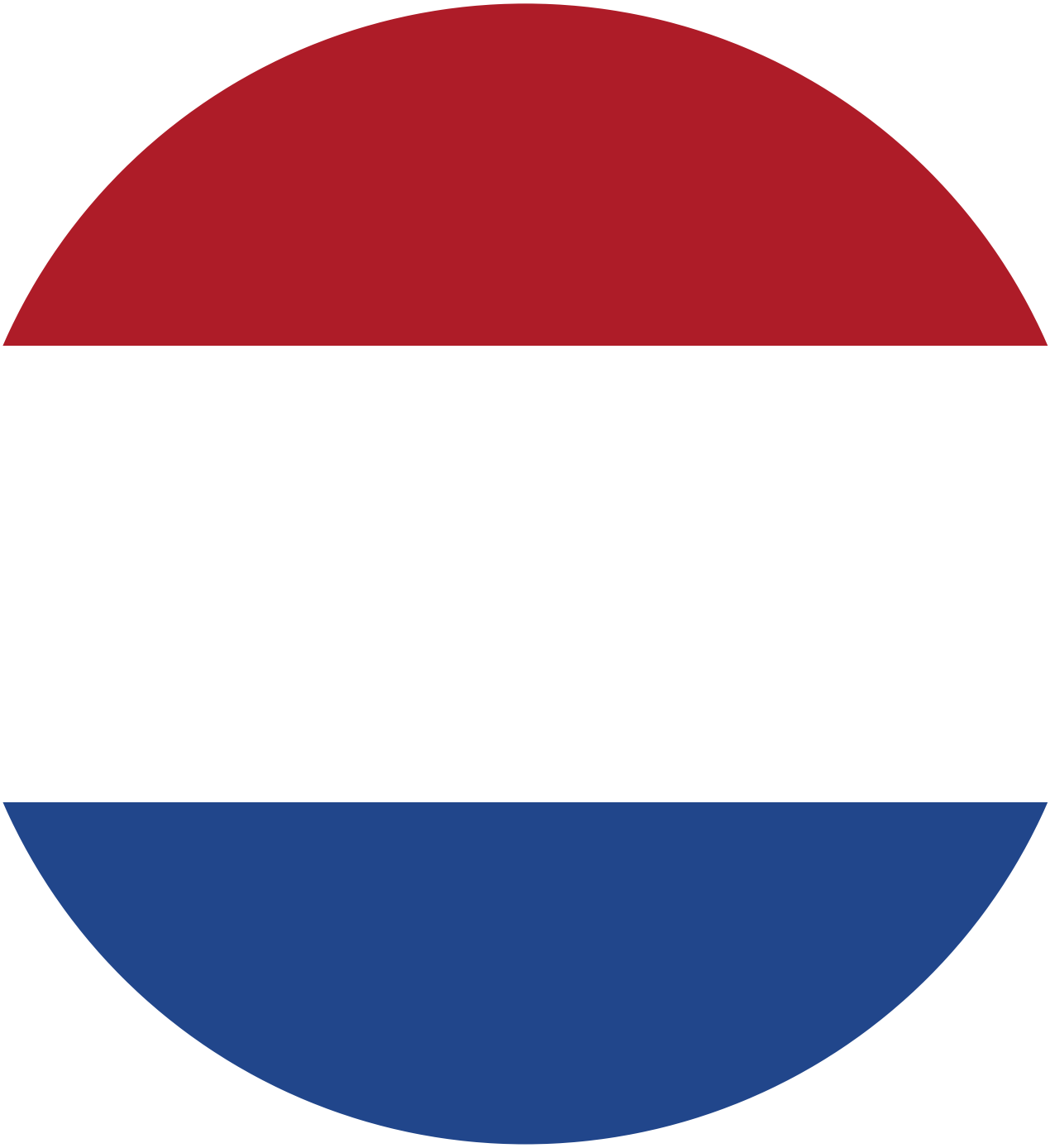
- France

- Belgique

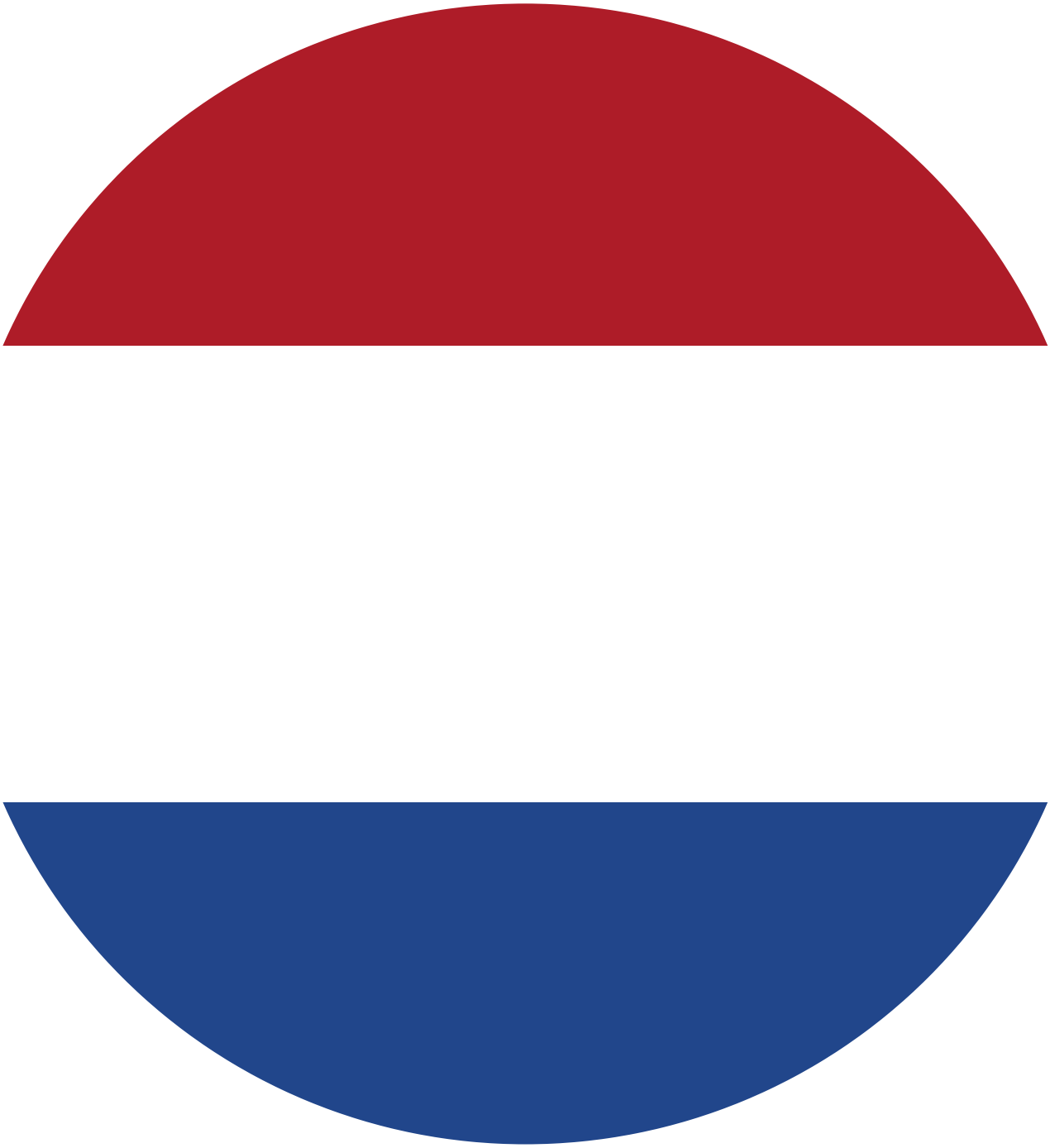
- België

- Suisse

- Schweiz



- Nederland



- Netherlands
- Deutschland
- Germany

- Österreich

SMARTER PARKING for SMART CITIES™

TERMS OF USE

In this Web Site Terms of Use ("TOU"), we, IPS Group Inc. set forth the terms by which you may use our site including www.ipsgroupinc.com and other web sites that we operate and on which we post a direct link to this statement (collectively the "Site"). By using the Site, you are agreeing to this TOU. If you do not agree to this TOU, you may not and should not use the Site.

1. **Copyright Notice and Use of the Site.** The contents of the Site are protected by the copyright and other laws of the United States, its treaty countries and other jurisdictions. Except as may otherwise be provided in a written Agreement you have with IPS Group Inc, you may not modify, copy, reproduce, republish, upload, post, transmit, transfer, or distribute in any way any of the contents of this site. You may download content from this site solely for your personal, non-commercial use (except as may otherwise be provided in a written agreement you have with IPS), provided you keep intact all copyright and other proprietary notices. Any copies of the content must include IPS's copyright notice: © Copyright 2005-2017 IPS Group Inc. All rights reserved.

2. **Links.** This website may contain links to third party web sites which are controlled and operated by third parties. Your use of each third party web site is subject to the terms of use and other guidelines, if any, contained within the relevant web site. You agree to review and accept such terms of use prior to using such third party web sites.IPS makes no representations whatsoever about any third party web site which you may access through the website. When you access a third party web site, you agree that it is independent from IPS, and that IPS has no control over any content on that web site. In addition, a link to a third party web site does not mean that IPS accepts any responsibility for the content, or the use, of such web

site. It is up to you to take precautions to ensure that whatever you select for your use is free of such items as viruses, worms, trojans and other items of a destructive nature.

3. Additional Terms for Forums, Blogs, and Other Social Media.Our Site may provide one or more forums, blogs, or other interactive or social media features ("Forums") for visitors to our Site to exchange information with each other and with IPS about IPS's products and services (the "Purpose"). If you use the Forums, in addition to any other terms we may require when you register to use the Forums or otherwise posted at or on the Forums, you agree to the following:

1. Restrictions. You agree not to use the Forums for any reason other than the Purpose. The material on the Forums is protected by international copyright and trademark laws. Except as permitted through a "Share" function which we may provide on the Forums (or with our express written permission), you may not modify, copy, reproduce, republish, upload, post, transmit, or distribute in any way any material from the Forums including any code or software we may provide.

2. Postings Not Necessarily the Opinion of IPS. Some of the individuals posting to Forums may work for IPS; however, opinions expressed here and in any corresponding comments are the personal opinions of the original authors, and do not necessarily reflect the views of IPS.

3. Postings. Although we may attempt to keep objectionable messages off the Site, it is impossible for us to review all messages. All messages express the views of the author, and IPS will not be held responsible for any message or associated content.If you post any messages, uploading files, inputting data, or engage in any other form of communication through the Forums (a "Posting"), you represent and warrant the following: (a) you own all right, title, and interest in and to the Posting, or you have been granted sufficient rights in and to the Posting allowing you to post such Posting, (b) you will not post any messages or other materials that are obscene, vulgar, sexually-orientated, hateful, threatening, or otherwise violate any laws, (c) you must not breach obligations of confidentiality that you owe to another party either in posting or using a Posting, (d) any Postings you make to the Site do not infringe any third party copyright, trade

marks, any other intellectual property rights or any applicable law and (e) you will indemnify us and our affiliates, partners, licensors, service providers, content providers, and their and our directors, officers, employees and agents against all claims, losses, liabilities, costs, damages and expenses incurred by us or them due to any breach by you of this TOU or your use of the Forums. For the purposes of this section, references to "your use" of the Forums shall be deemed to include any use by a third party where such third party accesses the Forums using your computer.You take full responsibility for any and all messages and associated content you post to the Forums or exchange through the Forums.When using the Forums and viewing Postings, you need to be aware of the following issues:

1. The Forums may include contributions from various sources over which IPS has no control (including any content submitted by third party users).
2. IPS does not pre-screen or exercise editorial control over Postings, and takes no responsibility for such Postings.
3. IPS reserves the right to edit or remove Postings at any time and in its sole discretion, including those that are in breach of this TOU or in breach of any obligation of confidentiality you owe IPS infringe or are alleged to infringe the intellectual property rights of any third party, or are defamatory, or otherwise are not relevant to the Forums and IPS will not be liable in relation to the removal of, or failure to remove, any Postings.

4. Messages to Registered Users. Our Forums may allow you to send messages directly to other Forum users who have made their contact information available for receiving such messages. You agree to only send messages to other Forum users for the purpose of exchanging information about the Purpose and any other use of the ability to send messages to other Forum users is strictly prohibited. Moreover, you shall not use the contact information made available through the Forum for any of the following: (1) to send unsolicited commercial email (i.e., spam) or any other type of unsolicited commercial message, or (2) to send any message that is vulgar, sexually-orientated, hateful, threatening, or otherwise violates any laws.

5. License. By adding a Posting to the Forum, you are granting IPS a royalty-free, perpetual, non-exclusive, unrestricted, worldwide license

to: (a) post, use, copy, sublicense, adapt, transmit, publicly perform or display any such Posting, (b) use, reproduce, modify, adapt, publish, translate, create derivative works from, distribute, perform, play, host, communicate, make available and publish your Posting without restriction and (c) sublicense to third parties the unrestricted right to exercise any of the foregoing rights granted with respect to the Posting. The foregoing grants shall include the right to exploit any ideas, concepts, intellectual property, or proprietary rights in such Posting, including but not limited to rights under copyright, trademark, servicemark or patent laws under any relevant jurisdiction without IPS owing any monies to you whatsoever.

6. IPS Employees. If you are a IPS employee, you must also follow the IPS Social Media Policy in your Postings.

7. Posting Guidelines. Our Forums may contain additional rules or posting guidelines. In such case, you agree to conform your Postings to any such additional rules or posting guidelines.

4. Privacy. In order to operate and provide the Site, we collect certain information about you. Our practices with respect to the information we collect is described in our privacy policy which is available at https://www.ipsgroupinc.com/privacy/ (“Privacy Policy”). By agreeing to this TOU you are agreeing to our Privacy Policy. Information, including but not limited to personal information, collected through the Site may be stored and processed in the United States or any other country in which IPS or its affiliates, subsidiaries or agents maintain facilities. By using the service, you consent to any such transfer of information outside of your country.

5. Disclaimer. The materials on the Site and on the Forums are provided “as is” and without warranties of any kind either express or implied. Commentary and other materials posted on the Site and Forums are not intended to amount to advice on which reliance should be placed and we therefore disclaim all liability and responsibility arising from any such reliance. To the fullest extent permissible pursuant to applicable law, IPS disclaims all warranties, express or implied, including, but not limited to, implied warranties of merchantability and fitness for a particular purpose, title and non-infringement and any other conditions, warranties and other terms which might otherwise be implied by statute, common law or the law of equity. IPS does not warrant that the Site or functions contained in

the materials will be uninterrupted or error-free, that defects will be corrected, or that the Site, or the server that makes it available, are free of viruses or other harmful components. IPS does not warrant or make any representations regarding the use or the results of the use of the materials on the Site in terms of correctness, accuracy, timeliness, reliability, or otherwise. You (and not IPS or its licensors) assume the entire cost of all necessary maintenance, repair, or correction.

6. Limitation of liability. Under no circumstances, including, but not limited to, negligence, shall IPS, its subsidiaries and parent companies and affiliates be liable for any direct, indirect, incidental, special or consequential damages that arise or result from or are related to the use of, or the inability to use, the Site or any of the Postings made available on or through the Site. Under no circumstances shall IPS's aggregate liability exceed $5.00. You specifically acknowledge and agree that IPS, its subsidiaries and parent companies and affiliates are not liable for any defamatory, offensive or illegal conduct of any user of the Site or any posting to the Site. If you are dissatisfied with the Site or any materials made available by or through the Site, or with this TOU, your sole and exclusive remedy is to discontinue using the Site.

7. Notices of copyright infringement. Notifications of claimed copyright infringement should be sent to IPS's Designated Agent in writing at the following address:

IPS Group Inc
Attn. Corporate Legal, Copyright Agent
7737 Kenamar Court
San Diego, CA 92121
Telephone Number of Designated Agent: (858) 634-2083
Facsimile Number of Designated Agent: (858) 404-0603
Email Address of Designated Agent: legal@ipsgroupinc.com
To be effective, the Notification must include the following:

- A physical or electronic signature of the owner whose exclusive right is allegedly infringed or a person authorized to act on his or her behalf;
- Identification of the copyrighted work claimed to have been infringed, or if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site;
- Identification of the material that is claimed to be infringing or is the subject of infringing activity and that is to be removed or access to

which is to be disabled, and information reasonably sufficient to permit IPS to locate the material on the Site;

- Information reasonably sufficient to permit IPS to contact the copyright owner or his/her authorized agent including an address, telephone number, and if available, an electronic mail address;
- A statement that the copyright owner or authorized agent has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law;
- A statement that the information in the notification is accurate, and if submitted by the owner's authorized agent a statement under penalty of perjury, that the agent is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.Within a commercially reasonable time after receipt of the written Notification containing the information as outlined in 1 through 6 above IPS shall remove or disable access to the material that is alleged to be infringing and forward the written notification to the alleged infringer and take reasonable steps to promptly notify the alleged infringer that IPS has removed or disabled access to the allegedly infringing material.Counter Notification: To be effective, a Counter Notification must be a written communication provided to IPS's Designated Agent at the above provided address that includes substantially the following:
- A physical or electronic signature of the alleged infringer;
- Identification of the material that has been removed or to which access has been disabled and the location at which the material appeared before it was removed or access to it was disabled;
- Astatement under penalty of perjury that the alleged infringer has a good faith belief that the material was removed or disabled as a result of a mistake or misidentification of the material to be removed or disabled;
- The alleged infringer's name, address, and telephone number, and a statement that the alleged infringer consents to the jurisdiction of Federal District Court for San Diego County, California, or if the Subscriber's address is outside of the United States, for any judicial district in which IPS may be found, and that the alleged infringer will accept service of process from the person who provided notification or an agent of such person.

After receipt of a Counter Notification containing the information as outlined in 1 through 4 above, IPS shall provide the Complaining Party with a copy of the Counter Notification within a commercially reasonable time and inform the copyright owner or designated agent that IPS will replace the removed material or cease disabling access to it within ten (10) business days. If IPS's designated agent has not received notice from the copyright owner or his/her designated agent within ten (10) business days that an action has been filed seeking a court order to restrain the alleged infringer from engaging in infringing activity in relation to the allegedly infringing material, IPS shall restore the allegedly infringing material.

EXPORT RESTRICTIONS.

ANY SOFTWARE OR OTHER MATERIALS WE MAKE AVAILABLE ON THE SITE ARE SUBJECT TO UNITED STATES EXPORT LAWS AND REGULATIONS. YOU MUST COMPLY WITH ALL DOMESTIC AND INTERNATIONAL EXPORT LAWS AND REGULATIONS THAT APPLY TO THE SOFWARE OR OTHER MATERIALS YOU OBTAIN FROM OUR SITE. THESE LAWS INCLUDE RESTRICTIONS ON DESTINATIONS, END USERS AND END USE.

Export Compliance Assurances.

You acknowledge that all products, proprietary data, know-how, software or other data or information (herein referred to as "Products") obtained from IPS or any direct Product thereof are subject to the United States (U.S.) government export control laws accordingly their use, export and re-export, may be restricted or prohibited. You and your affiliates agree to obtain prior to export an authorization from the applicable U.S. government agency (either in writing or as provided by applicable regulation). These U.S. government restrictions are implemented principally through the Export Administration Regulations ("EAR", 15 C.F.R. §§ 730 et seq., available at https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear) administered by Department of Commerce, Bureau of Industry and Security and the Foreign Asset Control Regulations administered by the Department of Treasury, Office of Foreign Assets

Control (“OFAC”, 30 C.F.R. Part 500 et. Seq. available at https://www.treasury.gov/resource-center/sanctions/CivPen/Pages/civpen-index2.aspx. You, therefore, agree that neither you nor your subsidiaries or affiliates will directly or indirectly export, re-export, transfer, or release, or cause to be exported or re-exported (herein referred to as “export”), any such Products or any direct Product thereof to any destination or entity prohibited or restricted under U.S. law including but not limited to U.S. government embargoed or sanctioned countries or entities, or nationals unless you shall obtain prior to export an authorization from the applicable U.S. government agency (either in writing or as provided by applicable regulation). You further agree that no Products received from IPS will be directly or indirectly employed in missile technology, sensitive nuclear, or chemical biological weapons end uses or in any manner transferred to any party for any such end use. This requirement shall survive any termination or expiration of this Agreement.

Trademarks.

IPS Group Logo and Next Revolution in Parking is a trademark of IPS Group Inc. Certain other product names, brand names and company names mentioned in this site may be trademarks of their respective owners.

Modification & Termination.

This TOU is effective until modified or terminated by IPS. IPS may modify this TOU from time to time and the new TOU will be effective when posted. IPS may also terminate this TOU at any time without notice to you. In the event of termination, you are no longer authorized to access the Site and the restrictions imposed on you with respect to material downloaded from the Site, the disclaimers and limitations of liabilities, and export restrictions set forth in this agreement, shall survive.

General.

This TOU shall be governed by and construed in accordance with the laws of the State of California without giving effect to any principles or

conflicts of law. If any provision of this TOU shall be unlawful, void or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions.

Effective:

September 30, 2015

MADE IN THE USA.
TRUSTED EVERYWHERE.

TERMS AND CONDITIONS

Last Updated: December 10, 2021

IMPORTANT NOTICE: THIS AGREEMENT CONTAINS A BINDING ARBITRATION PROVISION AND CLASS ACTION WAIVER. IT AFFECTS YOUR LEGAL RIGHTS AS DETAILED IN THE ARBITRATION AND CLASS ACTION WAIVER SECTION BELOW. PLEASE READ CAREFULLY.

These Terms and Conditions ("Terms") set forth a legally binding agreement between you and Passport Labs, Inc. and its corporate affiliates, subsidiaries, and divisions as may change from time to time (collectively, "Passport," "we," "us," and "our"). These Terms govern your access to and use of our websites, mobile applications (the "Apps" or each individually an "App"), and any other online services in which these Terms are displayed (collectively, the "Services"). Your access to and use of the Services are conditioned on your acceptance of and compliance with these Terms. By accessing or using the Services you, your heirs, assigns, and successors (collectively, "you" or "your") are indicating that you have read, understand, and agree to be bound by these Terms. If you do not agree to these Terms, then you must stop accessing or using the Services. If you are using the Services on behalf of a Partner (as defined below), that separate agreement shall control in the event of any conflict with these Terms; all other non-conflicting provisions in these Terms shall apply to your use of the Services.

The Services provided by Passport include transportation management services. Passport works with transit agencies, local governments and interlocal agencies or partnerships, tolling agencies, colleges, universities, hospital systems, and other public and private operators (each a "Partner" and collectively "Partners") to facilitate transportation management, such as parking and toll payment.

1 – Modifications

We may revise these Terms from time to time to reflect changes to the Services, our users' needs, the needs of our Partners, our business priorities, or changes in laws and regulations. The most current version will always be on this page. If the revision, in Passport's sole discretion, is material under applicable law, we will notify you via posting to our website or by other means in accordance with applicable legal requirements. Except as set forth in the "Arbitration and Class Action Waiver" Section below, or as otherwise provided by law, by continuing to access or use the Services after those revisions become effective, you agree to be bound by the revised Terms. The Terms were most recently updated on the last updated date listed at the top of this page.

2 – Additional Terms and Policies

Please review Passport's Privacy Policy, available at https://www.passportinc.com/privacy-policy/ and incorporated herein by reference (the "Privacy Policy"), for information and notices concerning Passport's collection, use, and disclosure of information collected through the Services. As set forth in the Privacy Policy, you acknowledge, consent, and agree that Passport may access, preserve, and disclose your information if we believe that it is (1) reasonably necessary to comply with any applicable law, regulation, subpoena, legal process or enforceable governmental request; (2) necessary to enforce the provisions of the Privacy Policy; (3) required to enforce our Terms, including investigation of potential violations; or (4) necessary to investigate or protect against actual or threatened harm to the rights, property, or safety of Passport, our users, or the public as required or permitted by law.

Passport offers various products, each of which may be governed by other terms as listed below in the "Product-Specific Terms" Section and displayed in the product. If there is a direct conflict

between these Terms and the terms displayed in another product offered by Passport, the latter takes precedence with respect to your use of that product.

3 – Eligibility and Scope

You may use the Services only if you can form a binding contract with Passport, and only in compliance with these Terms and all applicable local, state, national, and international laws, rules, and regulations. Without limiting the foregoing, the Services are only available to those who are at least 18 years old. If you're agreeing to these Terms on behalf of an organization or entity, you represent and warrant that you are authorized to agree to these Terms on that organization or entity's behalf and bind them to these Terms (in which case, the references to "you" and "your" in these Terms except for in this sentence, refer to that organization or entity).

If Passport has previously prohibited you from accessing or using the Services, you are not permitted to access or use the Services except as may subsequently be permitted in Passport's sole discretion.

4 – Account Registration

You may be required to register for a password-protected account ("Account") to use parts of the Services. You must provide accurate, current, and complete information during registration and at all other times when you use the Services, and update information to keep it accurate, current, and complete. Among other things, you may be required to add vehicles to your Account. By adding a vehicle, you represent and warrant that you are authorized to add such a vehicle to your Account, that all vehicles are registered and insured per applicable law, and that all drivers of such vehicle are properly licensed to operate such vehicle. We reserve the right to prohibit certain vehicles from being added to an Account. We may request additional information from you to authenticate your Account.

You are solely responsible for safeguarding your Account credentials and authentication measures, including your password or personal identification number ("PIN"). We encourage you to use a strong Account password or PIN. You are solely responsible for all activity that occurs on your Account, and we may assume that any activity under your Account has been initiated by you. You must notify Passport immediately of any breach of security or unauthorized use of your Account. Passport will not be liable, and you may be liable for losses, damages, liability, expenses, and lawyers' fees incurred by Passport or a third party arising from someone else using your Account

due to your conduct regardless of whether you have notified us of such unauthorized use. You understand and agree that we may require you to provide information that may be used to confirm your identity and help ensure the security of your Account.

5 – Rules and Prohibitions

The following requirements apply to your use of the Services:

- You will not use any feature of the Services, including chat features, for any purpose that is unlawful, tortious, abusive, intrusive on another's privacy, harassing, libelous, defamatory, embarrassing, obscene, threatening, or hateful.
- You will not use the Services for any commercial purpose not expressly approved by Passport in writing.
- You will not upload or otherwise transmit any material that contains viruses or any other computer code, files, or programs which might interrupt, limit, or interfere with the functionality of any computer software or hardware or telecommunications equipment.
- You will not rent, lease, lend, sell, sublicense, assign, distribute, publish, transfer or otherwise make available the Services or any features or functionality of the Services, to any third party for any reason.
- You will not remove, delete, alter, or obscure any trademarks or any copyright, patent or other intellectual property or proprietary rights notices from the Services, including any copy thereof.
- You will not use the Services in a way that violates any law or promotes any illegal activities, including, but not limited to the submission of inappropriate or unlawful content to or through the Services.
- You will not obtain or attempt to obtain unauthorized access to the Services or to Passport's servers, systems, network, or data; scrape, access in violation of these Terms, monitor, index, frame, link, copy, or search (or attempt to do so) the Services by any means (automated or non-automated) other than through currently available, published interfaces that are provided by Passport (and only pursuant to these Terms) (crawling the Services is permissible in accordance with these Terms, but scraping the Services without the prior written consent of Passport is expressly prohibited).
- You will not use another person's Account, impersonate any person or entity; or forge or manipulate headers or identifiers to disguise the origin of any content transmitted through the Services.
- You will not violate any rights of any third party, including trade secrets, privacy, or publicity rights.
- You will not undertake any activity or engage in any conduct that is inconsistent with the business or purpose of the Services or that would be intentionally deceitful or fraudulent.
- You will not probe, scan, or test the vulnerability of any system or network or breach or circumvent any security or authentication measures we may use to prevent or restrict access to the Services or use of the Services or the content therein.
- You will not attempt to indirectly undertake any of the prohibitions herein.

6 – Passport's License to You

Subject to your compliance with these Terms, Passport grants you a limited, non-exclusive, non-assignable, non-sublicensable, revocable, license to use the Services as it is provided to you by Passport. Except where Passport has explicitly agreed otherwise, the license granted herein is solely for your personal, noncommercial use. The license extends only in connection with your access to and participation in the Services and only in a manner that complies with all legal requirements that apply to you or your use of the Services.

Passport may revoke this license at any time, in its sole discretion. Upon revocation, you may not access or use the Services, and you must delete all copies of our App or other software from your devices. Neither title nor any intellectual property rights are transferred to you, but rather remain with Passport or its licensors, who own full and complete title, and Passport and respective licensors reserve all rights not expressly granted to you. You will not use, copy, adapt, modify, prepare derivative works based upon, distribute, license, sell, transfer, publicly display, publicly perform, transmit, stream, broadcast, or otherwise exploit the Services, except as expressly permitted in these Terms.

Passport further reserves the right to modify, suspend, or terminate the Services at any time in its sole discretion.

7 – Account Suspension or Termination

We may, in our discretion, with or without cause, with or without prior notice and at any time, decide to limit, block, suspend, deactivate, or cancel your Account in whole or in part. We may also temporarily or permanently prohibit you or any other user from adding a particular vehicle to an account. Without limiting the foregoing, we may terminate your Account if we suspect fraud, such as if you engage in excessive use of chargebacks on your payment method. If we exercise our discretion under these Terms to do so, any or all of the following can occur with or without prior notice or explanation to you: (a) your Account will be deactivated or suspended, your password or PIN will be disabled, and/or you will not be able to access the Services or receive assistance from Passport support teams; and (b) if appropriate in our sole discretion, we may communicate to third parties that your Account has been terminated, blocked, suspended, deactivated, or cancelled, and why this action has been taken. You may cancel your use of the Services and/or terminate your Account at any time by emailing support@passportinc.com. Please note that if your Account is cancelled, we do not have an obligation to delete or return to you any Account records or activity, unless otherwise required, and to the extent required, under applicable law.

8 – Proprietary Rights and Feedback

All right, title, and interest in and to the Services are and will remain the exclusive property of Passport and its licensors. All materials therein, including, without limitation, software, images, text, graphics, illustrations, logos, patents, trademarks, service marks, copyrights, photographs, audio, videos, music, and all intellectual property rights related thereto, are the exclusive property of Passport and its licensors. The Services are protected by copyright, trademark, and other laws of both the United States and foreign countries. You acknowledge that the Services have been developed, compiled, prepared, revised, selected, and arranged by Passport and others through the application of methods and standards of judgment developed and applied through the expenditure of substantial time, effort, and money and constitute valuable intellectual property of Passport and such others. Except as explicitly provided herein, nothing in these Terms gives you a right to use the Passport name or any of the Passport trademarks, logos, domain names and other distinctive brand features. Any other trademarks, service marks, logos, trade names and any other proprietary designations are the trademarks or registered trademarks of their respective owners.

Any feedback, comments, questions, or suggestions (collectively, “Feedback”) you may provide regarding the Services is entirely voluntary, and we will be free to use such feedback, comments or suggestions without any obligation to you. By sending us any Feedback, which may include via “app store” channels, such as the Apple App Store and Google Play Store, you further (i) agree that we are under no obligation of confidentiality, express or implied, with respect to the Feedback; (ii) acknowledge that we may have something similar to the Feedback already under consideration or in development; (iii) grant us an irrevocable, non- exclusive, royalty-free, perpetual, worldwide license to use, modify, prepare derivative works, publish, distribute, and sublicense the Feedback; and (iv) irrevocably waive, and cause to be waived, against Passport any claims and assertions of any moral rights contained in such Feedback. These provisions regarding Feedback shall survive any termination of your Account or the Services.

9 – Payments

Our Services may require payments from you, such as when you use the Services to pay for parking, tolls, or transportation fares, or where we offer you the ability to pay citations or purchase permits through the Services. The payment required shall be displayed to you through the Services. You understand that only certain forms of payment may be accepted, and these acceptable forms of payment are subject to change at any time. You may provide us with a method of payment, and by doing so, you represent and warrant that you are authorized to use that method of payment.

You are responsible for all activity in your Account, including payment transactions. When a payment transaction is initiated in your Account, you authorize us to process the applicable fees by charging any payment method you provide us or deducting the fees from any funds you have stored with us (see Section 10 below on Passport Wallet). You may also be given the option to prioritize the order in which your payment methods are charged. If you do not have a valid form of payment transaction, you will not have access to all Services. We also reserve the right to suspend or terminate your Account if your payment method is declined or if we suspect any fraud on your Account. If you have stored payment information with us, you agree to keep such payment information accurate, current, and complete. We are not responsible if your access to the Services is limited based on inaccurate payment information.

We use a third-party payment provider for processing payment transactions. The third-party payment provider may impose insufficient funds, charges or other fees. We are not responsible for your interactions with third-party payment providers or for any charges or fees they may impose. When you use any of the Services that require payment, a temporary pre-authorization hold may be placed on your designated payment method to verify that the card is valid and has funds available for your intended purchase. The amount of this pre-authorization hold may be greater or less than the order total for your transaction. Your payment will be captured up to 24 hours after your order is completed or cancelled. In the event that the pre-authorization is greater than the final amount, the difference will be released after your order is completed or cancelled; depending on your bank, it may take up to 5 Business Days to receive access to these released funds. If your payment details change, your card provider may provide us with updated card details. We may use these new details in order to help prevent any interruption to your use of the Services. If you would like to use a different payment method or if there is a change in payment method, please visit your account settings to update your billing information.

10 – Passport Wallet

a. How it Works

We may offer you an option to store funds with us for use in our Services (“Passport Wallet”). Passport Wallet may be offered on an auto-reloading basis. If you register for an auto-reloading Passport Wallet (“Auto-Reload Wallet”), you acknowledge and agree that when the available funds in your Passport Wallet equal or drop below a designated balance (“Designated Reload Balance”), we may automatically add funds to your Passport Wallet (“Preset Wallet Reload Amount”) by charging the payment method you have provided us. We will send you an email confirming each

Auto-Reload Wallet transaction or otherwise make your transaction history available within the Services. The automatic charges will stop when: (a) your Account terminates; (b) you or Passport cancel the Auto-Reload Wallet feature (provided, however, that canceling the Auto-Reload Wallet may make use of the Services impractical or impossible); or (c) these Terms are otherwise properly terminated as expressly permitted herein.

Depending on the types of Services you use, you may be able to change the Designated Reload Balance or Preset Wallet Reload Amount or cancel the Auto-Reload Wallet feature by accessing the settings in your Account. Note that changes may take up to 24 hours to take effect. Please be advised that we may be required by our Partners to impose a minimum and/or maximum amount of the Designated Reload Balance or Preset Wallet Reload Amount, and we may designate different minimum/maximum amounts depending on your payment history and payment method, our contractual obligations with our Partners, or for any other reason in our sole discretion. For example, we may require that you maintain at least $20 in your Passport Wallet. We may also designate required denominations of the Designated Reload Balance. If you do not agree, you may not use the Auto-Reload Wallet feature. We will notify you if the Designated Reload Balance or Preset Wallet Reload Amount you previously designated is no longer accepted. You will not receive interest or other earning on the funds in your Passport Wallet.

You authorize us and/or our third-party payment providers to store your payment method for the purpose of the Auto-Reload Wallet feature, where applicable, and you authorize us (without notice to you, unless required by law), to charge fees against that payment method to replenish funds in your Passport Wallet. For example, fees may be charged when your Passport Wallet falls below a certain threshold, as designated when you register for the Auto-Reload Wallet. Please be advised that some services may require your participation in the Auto-Reload Wallet feature.

If we are unable to complete your Auto-Reload Wallet charge with the payment method you previously selected, you authorize us to add funds to your Passport Wallet by charging another payment method associated with your account, where available. If the funds in your Passport Wallet equal or drop below the Designated Reload Balance and we are unable to complete the Auto-Reload Wallet charge, we may disable your Passport Wallet and/or otherwise limit your use of the Services. Additionally, if you have a negative balance in your Passport Wallet (i.e., you owe money), and your Preset Wallet Reload Amount does not suffice to bring your Passport Wallet out of a negative balance, we reserve the right to adjust the Preset Wallet Reload Amount to recover funds you owe or to charge the Preset Wallet Reload Amount twice or more as necessary to cure the negative balance.

If you maintain a Passport Wallet, you may also have access to promotional codes or other benefits such as a discounted parking session. We may also offer promotions that effectively provide a discount to you when you load funds into your Passport Wallet. Additional terms and fees may apply as indicated within the Services.

If you dispute any of the payments made through our Services, we may direct you to the applicable Partner if such Partner is responsible for front-line support. In that case, please be advised that we provide only a platform for connecting you to our Partners who provide transportation-related services.

b. Lost Access Credentials and Unauthorized Activity

You agree to notify us immediately at (704) 837-8066 or support@passportinc.com if you believe the access credentials used to access your Account ("Access Credentials") have been compromised, or if you believe that a transfer has been made without your permission using information about your Account. Calling us is the best way of keeping your possible losses down. You could lose all the money in your Account. If you fail to notify us within 2 Business Days, you may face greater losses. "Business Days" means Monday through Friday, not including any legal holidays.

You agree to notify us immediately at (704) 837-8066 or support@passportinc.com if your Account shows transfers you did not authorize. Notifications must include the information identified below to be effective. Without limiting your duty to notify us immediately, such notification must be made no later than 60 days after the date after the date of the unauthorized transfer. You may not recover the unauthorized amounts transferred if you fail to notify us within 60 days after the date of the unauthorized transfer, and we can prove that we could have stopped someone from taking the money if you had notified us in time. If a good reason (such as a long trip or a hospital stay) kept you from telling us, we may extend the time periods.

To notify us of unauthorized transfers or to otherwise request more information about a transfer listed on the statement or receipt, call us at (704) 837-8066, email us at support@passportinc.com, or write to us at 128 S. Tryon St., Suite 2200, Charlotte, NC 28202 (or such other contact information as might be listed on the statement or receipt).

We will need:

- Your name and Account identifier;

- A description of the error or the transfer you are unsure about, and explain as clearly as you can why you believe it is an error or why you need more information; and
- The dollar amount of the suspected error.

If you notify us via a phone call to (704) 837-8066, you agree to send your complaint or question in writing to us within 10 Business Days if we request it. Failure to do so may result in us being unable to process your request, and we may not credit your Account. Except as provided herein, we will determine whether an error occurred, and correct any such error, promptly and within any applicable time period required by law. If we need more time to conduct our investigation, however, we will notify you of our need for an extension to investigate your complaint or question which may be up to the maximum period allowed under applicable law. If we decide to do this, we will credit your Account to the extent required by applicable law for the amount you think is in error, so that you will have the use of the money during the time it takes us to complete our investigation.

For errors involving new accounts or point-of-sale transactions we may take a longer period, up to the maximum period allowed under applicable law, to investigate your complaint or question and to credit your account for any amount you think is in error. We will tell you the results promptly after completing our investigation and within any time periods required by applicable law. If we decide that there was no error, we will send you an explanation. You may ask for copies of the documents that we used in the investigation.

c. Transfer Types and Limitations

You may use the Services to fund your Account and to pay for transit services at participating locations for the vehicle(s) associated with your Account. We will not limit the number of purchases of Services you may make, but for security reasons we may limit the amount of funds you may load into your Account.

d. Account Statements

We will send you statements for your Account by electronic mail or by posting through the Services. You may contact the number listed on the statement for your Account or in the Services for any inquiries relating to your Account history.

e. Fees

Fees will be made available within the Apps.

f. Our Liability

If we do not complete a transfer to or from your Account on time or in the correct amount according to our agreement with you, our liability to you will be as provided by applicable law and subject to our agreement with you. However, we will not be liable, for instance:

- If not required by law;
- If, through no fault of ours, you do not have enough money in your Account to make the transfer;
- If the Services were not working properly and you knew about such issue(s) when you started the transfer;
- If circumstances beyond our control prevent the transfer, despite reasonable precautions that we have taken;
- Any other exception permitted in our agreements with you.

g. Closed Accounts and Refunds

If you close your Account, unless you owe fees, we will provide you with a refund of any amounts remaining in your Passport Wallet. We may, for example, request your mailing address so we can send you a refund check by mail. We are not responsible for failed deliveries of any refund check, e.g. if you provide us with the wrong mailing address or do not update your mailing address with us. Please allow up to 6 weeks for a refund. We will refund the money to the payment method you designated, by check, or as otherwise deemed reasonable in our discretion. Except as provided herein, Passport Wallet funds are not refundable.

11 – Text Messaging

Some of the services we provide, such as when you use our Services to pay for parking, may offer you the ability to manage transactions through text messages. For example, if you initiate a parking transaction by calling or sending us a text message to the phone number associated with that parking location, you expressly consent to receive text messages relating to that transaction at the phone number from which you communicated with us. You understand that message and data rates may apply, and we are not responsible for payment of such fees. If you do not want to receive text messages, please do not initiate a parking transaction by calling or sending us a text message. For example, you may initiate a parking transaction through the App instead. We are not responsible for any text messages that fail to be delivered to you, including where your device is on a network not supported by us or our vendors. To stop receiving these parking transaction text messages, you must reply “STOP” to one of our text messages. We may send you a text message

confirming your opt-out. To opt back into receiving text messages, you can initiate another parking transaction by calling or sending us a text message to the phone number associated with that parking location.

12 – Third-Party Links and Resources

The Services may contain information and content provided by third parties and may contain links to third-party websites, mobile applications, software, and other resources that are not owned or controlled by Passport, including those maintained by governmental entities ("Third-Party Resources"). Passport is not responsible for the availability, accuracy, content, products, or services of such Third-Party Resources and does not endorse and is not responsible or liable for such Third-Party Resources. These links and resources do not imply any endorsement by Passport, and Passport does not endorse or assume any responsibility for any such Third-Party Resources. If you access a Third-Party Resource from the Services, including websites, mobile applications, or resources maintained by governmental entities, you do so at your own risk, and you understand that these Terms and the Privacy Policy do not apply to your use of such Third-Party Resources. You understand that your use of Third-Party Resources may be subject to terms and conditions imposed by third parties. You expressly relieve Passport from any and all liability arising from your use of any Third-Party Resources. You acknowledge and agree that Passport is not responsible or liable for: (i) the availability or accuracy of such Third-Party Resources; or (ii) the content, products, or services on or available from such Third-Party Resources.

13 – Warranties and Disclaimers

Your access to and use of the Services is at your own risk. You understand and agree that the Services are provided to you on an "AS IS" and "AS AVAILABLE" basis. Without limiting the foregoing, PASSPORT AND ITS AFFILIATES AND SUBSIDIARIES, AND THEIR RESPECTIVE OFFICERS, DIRECTORS, EMPLOYEES, AND AGENTS DISCLAIM ANY WARRANTIES, EXPRESS OR IMPLIED, OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, QUIET ENJOYMENT, OR NON-INFRINGEMENT. We make no warranty and disclaim all responsibility and liability for the completeness, accuracy, availability, timeliness, security, or reliability of the Services or any content thereon. Passport will not be responsible or liable for any harm to your computer system, loss of data, or other harm that results from your access to or use of the Services. You also agree that Passport has no responsibility or liability for its deletion of, or the failure to store, retain, or transmit, any records related to your Account. We make no warranty that the Services will meet your requirements or be available on an uninterrupted, secure, or error-free basis. No advice or

information, whether oral or written, obtained from Passport or through the Services, will create any warranty not expressly made herein.

The Services are controlled and operated from Passport's facilities in the United States. Passport makes no representations that the Services are appropriate or available for use in locations other than the United States, Canada, or the United Kingdom. Those who access or use the Services from other jurisdictions do so at their own volition and are entirely responsible for compliance with all applicable United States and local laws and regulations, including but not limited to export and import regulations. You may not use the Services if you are a resident of a country embargoed by the United States, or are a foreign person or entity blocked or denied by the United States government. Unless otherwise explicitly stated, all materials found on the Services are solely directed to individuals, companies, or other entities located in the United States, Canada, and the United Kingdom.

14 – Limitation of Liability

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, PASSPORT AND ITS AFFILIATES AND SUBSDIARIES, AND THEIR RESPECTIVE OFFICERS, EMPLOYEES, AGENTS, PARTNERS AND LICENSORS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR PUNITIVE DAMAGES, INCLUDING WITHOUT LIMITATION, LOSS OF PROFITS, DATA, USE, GOOD-WILL, OR OTHER INTANGIBLE LOSSES, RESULTING FROM (i) YOUR ACCESS TO OR USE OF OR INABILITY TO ACCESS OR USE THE SERVICES; (ii) ANY CONDUCT OR CONTENT OF ANY THIRD-PARTY RESOURCES; (iii) ANY CONTENT OBTAINED FROM THE SERVICES; AND (iv) UNAUTHORIZED ACCESS, USE OR ALTERATION OF YOUR TRANSMISSIONS, WHETHER BASED ON WARRANTY, CONTRACT, TORT (INCLUDING NEGLIGENCE) OR ANY OTHER LEGAL THEORY, WHETHER OR NOT PASSPORT HAS BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGE, AND EVEN IF A REMEDY SET FORTH HEREIN IS FOUND TO HAVE FAILED OF ITS ESSENTIAL PURPOSE.

THE LIMITATION OF LIABILITY DESCRIBED ABOVE SHALL APPLY FULLY TO RESIDENTS OF NEW JERSEY.

Some jurisdictions do not allow the exclusion of certain warranties or the exclusion or limitation of liability for consequential or incidental damages, so the limitations above may not apply to you.

15 – Indemnification

TO THE FULL EXTENT PERMITTED BY LAW, YOU AGREE TO RELEASE, DEFEND, INDEMNIFY, AND HOLD PASSPORT AND ITS AFFILIATES AND SUBSIDIARIES, AND THEIR RESPECTIVE OFFICERS, DIRECTORS, EMPLOYEES AND AGENTS, HARMLESS FROM AND AGAINST ANY CLAIMS, LIABILITIES, DAMAGES, LOSSES, AND EXPENSES, INCLUDING WITHOUT LIMITATION REASONABLE LEGAL AND ACCOUNTING FEES, ARISING OUT OF OR IN ANY WAY CONNECTED WITH (A) YOUR VIOLATION OF THESE TERMS; (B) YOUR VIOLATION OF ANY LOCAL, STATE, FEDERAL, OR INTERNATIONAL LAW, RULE, OR REGULATION; (C) ANY MISREPRESENTATION MADE BY YOU; OR (D) YOUR AUTHORIZATION OF ANYONE ELSE TO USE YOUR PASSWORD OR ACCOUNT.

If you are a California resident, you hereby waive California Civil Code § 1542, which says: “A general release does not extend to claims that the creditor or releasing party does not know or suspect to exist in his or her favor at the time of executing the release and that, if known by him or her, would have materially affected his or her settlement with the debtor or released party.” This release includes the criminal acts of others. If you are not a California resident, you waive your rights under any statute or common law principle similar to Section 1542 that governs your rights in the jurisdiction of your residence.

16 – Product-Specific Terms

Passport provides a number of different products and services. The following additional terms and conditions govern your use of these products.

a. Cashless Parking Services

The Cashless Parking Services enables you to pay for certain parking through our Services. You can activate the Cashless Parking Services for a particular parking transaction by either (1) using the App; (2) calling a phone number provided at the parking site (where available); (3) initiating a transaction via text messaging (where available), or (4) accessing our mobile website.

You are solely responsible for correctly entering the relevant parking zone number and space number, which will be displayed at the parking site; and license plate number where required. The parking zone number informs us of the rate to charge you for your parking at that parking site. It also informs us of any restrictions on the amount of time you are permitted to park your vehicle in that zone. You are responsible for checking the parking site to determine if there are other parking restrictions (“On-Site Parking Restrictions”). On-Site Parking Restrictions may include notices, signs, or directions posted by relevant Partners. We do not and cannot guarantee that the charges

displayed in our Services adequately account for On-Site Parking Restrictions. Any violations of On-Site Parking Restrictions are solely your responsibility.

Use of the Cashless Parking Services does not guarantee you a parking space, and you may only initiate the Cashless Parking Services after you have parked in an available space at that parking site. Before leaving your vehicle unattended, please confirm that we have accepted your parking transaction request. Confirmation shall be sent to you by text message (where you initiate a transaction by calling or sending us a text message) or through your App. You are responsible for any fine, ticket, or penalty charge issued between the time you park your vehicle and when you receive confirmation that we have accepted your parking transaction request.

You are solely responsible for resolving with the relevant authorities any issues that you may have regarding the issuance of fines, parking tickets, penalty notices or your vehicle being impounded.

b. Citations Services

The Citations Services enable you to pay for certain citations issued by government municipalities and, where available, appeal them.

To access your citation, you will be required to enter certain information, such as your license plate number or citation number. Please be advised that we provide only a platform for you to view and/or pay citations. We are not responsible for the issuance of citations, the validity or legality of such citations, the due date for payment of the citation, or the amount of any fees in citations. To the extent you have questions about your citation, you must do so via the contact information supplied on the citation. You are solely responsible for resolving with the relevant authorities any issues that you may have regarding the issuance of citations.

c. Parking Permitting Services

The Permitting Services enable you to obtain and manage certain parking-related permits issued by our applicable Partners. You will be required to provide us with certain information to obtain a permit, such as the license plate number of your vehicle. Permits issued through the Permitting Services are not transferable.

You understand that permits obtained through the Services may be subject to additional restrictions set by the applicable Partner. For example, permits may be issued specific to a single

vehicle. Likewise, applicable third parties may also impose policies that prohibit Passport from issuing refunds or exchanges of permits. You must keep the information in your Account and/or with that permit current and accurate, or you may be subject to penalties or fines imposed by regulatory authorities or third parties. You are responsible for any fine, ticket, or penalty charge issued for failure to comply with any permit terms, including terms imposed by government municipalities or other third parties.

d. Mobile Ticketing Services

The Mobile Ticketing Services enable you to pay certain fares associated with transportation services, such as bus and rail system fares. You must use our mobile ticketing Apps to access the Mobile Ticketing Services. Payment for Mobile Ticketing Services may be on a pay-per-use basis, in which case we would charge your payment method separately for each fare, or you may purchase and manage passes through the Services; the available fare and pass options will depend on the applicable Partner. Depending on the setup with our mobile ticketing Partners, you may be permitted to purchase multiple tickets, store them in your account, and redeem them as they are used. Some Partners may offer discounted fares, such as student or senior fares. By purchasing or redeeming tickets on these discounted fares, you represent and warrant that you qualify for such fares, and you may have to verify eligibility pursuant to our Partners' requirements. The Mobile Ticketing Services you utilize may contain additional rules and prohibitions. You are responsible for any fine, ticket, or penalty charge issued for failure to comply with such rules and prohibitions.

17 – Arbitration and Class Action Waiver

PLEASE READ THIS SECTION CAREFULLY. IT AFFECTS YOUR LEGAL RIGHTS, INCLUDING YOUR RIGHT TO FILE A LAWSUIT IN COURT.

You and Passport agree that these Terms affect interstate commerce and that the Federal Arbitration Act governs the interpretation and enforcement of these arbitration provisions.

This Section is intended to be interpreted broadly and governs any and all disputes between us, including but not limited to claims arising out of or relating to any aspect of the relationship between us, whether based in contract, tort, statute, fraud, misrepresentation or any other legal theory; claims that arose before these Terms or any prior agreement (including, but not limited to, claims related to your use of the Services, including payments initiated through the Services or your use of Passport Wallet); and claims that may arise after the termination of these Terms or

agreement to arbitrate. The only disputes excluded from this broad prohibition are the litigation of certain intellectual property and small court claims, as provided below.

By agreeing to these Terms, you agree to resolve any and all disputes with Passport as follows:

Initial Dispute Resolution: Most disputes can be resolved without resort to litigation. You can reach Passport's support department at support@passportinc.com. Except for intellectual property and small claims court claims, the parties agree to use their best efforts to settle any dispute, claim, question, or disagreement directly through consultation with the Passport support department, and good faith negotiations shall be a condition to either party initiating a lawsuit or arbitration.

Binding Arbitration: If the parties do not reach an agreed-upon solution within a period of 30 days from the time informal dispute resolution is initiated under the Initial Dispute Resolution provision above, then either party may initiate binding arbitration as the sole means to resolve claims, subject to the terms set forth below. Specifically, all claims arising out of or relating to these Terms (including the Terms' or the Privacy Policy's formation, performance, and breach), the parties' relationship with each other, and/or your use of the Services shall be finally settled by binding arbitration administered by JAMS in accordance with the JAMS Streamlined Arbitration Procedure Rules for claims that do not exceed $250,000 and the JAMS Comprehensive Arbitration Rules and Procedures for claims exceeding $250,000 in effect at the time the arbitration is initiated, excluding any rules or procedures governing or permitting class actions. The arbitrator, and not any federal, state, or local court or agency, shall have exclusive authority to resolve all disputes arising out of or relating to the interpretation, applicability, enforceability, or formation of these Terms or the Privacy Policy, including but not limited to any claim that all or any part of these Terms or the Privacy Policy is void or voidable, whether a claim is subject to arbitration, or the question of waiver by litigation conduct. The arbitrator shall be empowered to grant whatever relief would be available in a court under law or in equity. The arbitrator's award shall be written and shall be binding on the parties and may be entered as a judgment in any court of competent jurisdiction. To start an arbitration, you must do the following: (a) write a Demand for Arbitration that includes a description of the claim and the amount of damages you seek to recover (you may find a copy of a Demand for Arbitration at www.jamsadr.com); (b) send three copies of the Demand for Arbitration, plus the appropriate filing fee, to JAMS at 1155 F Street, NW, Suite 1150, Washington, DC 20004; and (c) send one copy of the Demand for Arbitration to the attention of Passport Legal Department at 128 S. Tryon St., Suite 2200, Charlotte, NC 28202.

You will be required to pay $250 to JAMS to initiate an arbitration against us. If the arbitrator finds the arbitration to be non-frivolous, Passport will pay all other fees invoiced by JAMS, including filing fees and arbitrator and hearing expenses. You are responsible for your own attorneys' fees unless the arbitration rules and/or applicable law provide otherwise.

The parties understand that, absent this mandatory arbitration provision, they would have the right to sue in court and have a jury trial. They further understand that, in some instances, the costs of arbitration could exceed the costs of litigation and the right to discovery may be more limited in arbitration than in court.

If you are a resident of the United States, arbitration may take place in the county where you reside at the time of filing. For individuals residing outside the United States, arbitration shall be initiated in the State of North Carolina, United States of America. You and Passport further agree to submit to the personal jurisdiction of any federal or state court in Mecklenburg County, North Carolina in order to compel arbitration, to stay proceedings pending arbitration, or to confirm, modify, vacate, or enter judgment on the award entered by the arbitrator.

Class Action Waiver: The parties further agree that the arbitration shall be conducted in their individual capacities only and not as a class action or other representative action, and the parties expressly waive their right to file a class action or seek relief on a class basis. **YOU AND PASSPORT AGREE THAT EACH MAY BRING CLAIMS AGAINST THE OTHER ONLY IN YOUR OR ITS INDIVIDUAL CAPACITY, AND NOT AS A PLAINTIFF OR CLASS MEMBER IN ANY PURPORTED CLASS OR REPRESENTATIVE PROCEEDING**. If any court or arbitrator determines that the class action waiver set forth in this paragraph is void or unenforceable for any reason or that an arbitration can proceed on a class basis, then the arbitration provisions set forth above shall be deemed null and void in their entirety and the parties shall be deemed to have not agreed to arbitrate disputes.

Exception: Litigation of Intellectual Property and Small Claims Court Claims: Notwithstanding the parties' decision to resolve all disputes through arbitration, either party may bring enforcement actions, validity determinations or claims arising from or relating to theft, piracy or unauthorized use of intellectual property in state or federal court or in the U.S. Patent and Trademark Office to protect its intellectual property rights ("intellectual property rights" means patents, copyrights, moral rights, trademarks, and trade secrets, but not privacy or publicity rights). Either party may also seek relief in a small claims court for disputes or claims within the scope of that court's jurisdiction.

30-Day Right to Opt Out: You have the right to opt out and not be bound by the arbitration and class action waiver provisions set forth above by sending (from the email address you used to register for your Account) written notice of your decision to opt out to classactionoptout@passportinc.com with the subject line, "ARBITRATION AND CLASS ACTION WAIVER OPT-OUT." The notice must be sent 30 days of your first use of the Services or the effective date of the first set of Terms containing an Arbitration and Class Action Waiver section, whichever is later; otherwise, you shall be bound to arbitrate disputes in accordance with the terms of these paragraphs. If you opt out of these arbitration provisions, Passport also will not be bound by them.

Changes to This Section: Passport will provide 30 days' notice of any changes affecting the substance of this section by posting on the Services, sending you a message, or otherwise notifying you when you are logged into your Account. Amendments will become effective 30 days after they are posted on the Services or sent to you.

Changes to this Section will otherwise apply prospectively only to claims arising after the 30th day. If a court or arbitrator decides that this subsection on "Changes to This Section" is not enforceable or valid, then this subsection shall be severed from the section entitled "Arbitration and Class Action Waiver," and the court or arbitrator shall apply the first Arbitration and Class Action Waiver section in existence after you began using the Services.

Survival: This "Arbitration and Class Action Waiver" Section shall survive any termination of your Account or the Services.

18 – General

Governing Law. You agree that: (i) the Services shall be deemed solely based in North Carolina; and (ii) the Services shall be deemed a passive one that does not give rise to personal jurisdiction over Passport, either specific or general, in jurisdictions other than North Carolina. These Terms shall be governed in all respects by the internal substantive laws of Delaware, without regard to its conflict of laws principles. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Except for claims that must be arbitrated pursuant to the "Arbitration and Class Action Waiver" Section, any claim or dispute arising in connection with the Services shall be decided exclusively by a court of competent jurisdiction located in Mecklenburg County, North Carolina, and you consent to the personal jurisdiction of and venue in such courts and waive any and all jurisdictional and venue defenses or objections otherwise available.

Entire Agreement. These Terms, together with the Privacy Policy and any other legal notices, amendments, and additional agreements or policies published by Passport on the Services, shall constitute the entire agreement between you and us concerning the Services. Except as set forth in the "Arbitration and Class Action Waiver" Section, if any provision of these Terms is deemed invalid by a court of competent jurisdiction, the invalidity of such provision shall not affect the validity of the remaining provisions of these Terms, which shall remain in full force and effect. These Terms supersede and replace any prior agreements between Passport and you regarding the Services.

Section Headings. The Section headings in these Terms are for convenience only and have no legal or contractual effect.

Waiver. No waiver of any term of this Agreement shall be deemed a further or continuing waiver of such term or any other term, and Passport's failure to assert any right or provision under these Terms shall not constitute a waiver of such right or provision.

Statute of Limitations. Except where prohibited by applicable law in your state or country of residence, such as New Jersey, you agree that regardless of any statute or law to the contrary, any claim or cause of action arising out of or related to use of the Services or these Terms must be filed within one year after such claim or cause of action arose or be forever barred.

Force Majeure. Neither Passport nor you shall be liable to the other for any delay or failure in performance under the Terms arising out of a cause beyond its control and without its fault or negligence. Such causes may include but are not limited to fires, floods, earthquakes, strikes, unavailability of necessary utilities, blackouts, acts of God, acts of declared or undeclared war, acts of regulatory agencies, or national disasters.

No Third-Party Beneficiaries. You agree that, except as otherwise expressly provided in these Terms, there shall be no third-party beneficiaries to these Terms.

Transferability and Assignability. These Terms, and any rights and licenses granted hereunder, may not be transferred or assigned by you, but may be assigned by Passport without restriction. Any attempted transfer or assignment in violation hereof shall be null and void. These Terms bind and inure to the benefit of each party and the party's successors and permitted assigns.

Notices. We may deliver notice to you by email, posting a notice on the Services, or any other method we choose, and such notice will be effective on dispatch. You agree to keep your email

address information current. You agree that all notices, disclosures, and other communications that we provide to you electronically satisfy any legal requirement that such communications be in writing. If you give notice to us, it will be effective when received by mail at 128 S. Tryon St., Suite 2200, Charlotte, NC 28202.

Contact us. Please contact us in writing at support@passportinc.com or 128 S. Tryon St., Suite 2200, Charlotte, NC 28202 with any questions regarding these Terms.

19 – Apple Terms

If the Services that you use include a mobile application that you download, access and/or use and that runs on Apple's iOS operating system (an "iOS App"), you acknowledge and agree that:

- the iOS App may only be accessed and used on a device owned or controlled by you and using Apple's iOS operating system and subject to Apple's usage rules and requirements;
- these Terms are between you and Passport, and not with Apple;
- Apple is not responsible for the Services and the content therein;
- Apple has no obligation at all to provide any support or maintenance services in relation to the iOS App, and if you have any maintenance or support questions in relation to the iOS App, please contact Passport, not Apple;
- except as otherwise expressly set forth in these Terms, any claims relating to the possession or use of the iOS App are between you and Passport (and not between you, or anyone else, and Apple);
- in the event of any claim by a third party that your possession or use (in accordance with these Terms) of the iOS App infringes any intellectual property rights, Apple will not be responsible or liable to you in relation to that claim; and
- although these Terms and Conditions are entered into between you and Passport (and not Apple), Apple, as a third-party beneficiary under these Terms and Conditions, will have the right to enforce them against you.

In addition, you represent and warrant that:

- you are not, and will not be, located in any country that is the subject of a United States Government embargo or that has been designated by the United States Government as a "terrorist supporting" country; and
- you are not listed on any United States Government list of prohibited or restricted parties; and
- if the iOS App does not conform to any warranty applying to it, you may notify Apple, which will then refund the purchase price of the iOS App (if any) to you. Subject to that, and to the maximum extent permitted by law, Apple does not give or enter into any warranty, condition or other term in relation to the iOS App and will not be liable to you for any claims, losses, costs or expenses of whatever nature in relation to the iOS App or as a result of you or anyone else using the iOS App or relying on any of its content.

20 – Google Terms

If the Services that you use include a mobile application that you download, access, and/or use from the Google Play Store ("Google-Sourced Software"): (i) you acknowledge that these Terms are between you and Passport only, and not with Google, Inc. ("Google"); (ii) your use of Google-Sourced Software must comply with Google's then-current Google Play Store Terms of Service; (iii) Google is only a provider of the Google Play Store where you obtained the Google-Sourced Software; (iv) Passport, and not Google, is solely responsible for its Google-Sourced Software; (v) Google has no obligation or liability to you with respect to Google-Sourced Software or the Terms; and (vi) you acknowledge and agree that Google is a third party beneficiary to the Terms as it relates to Passport's Google-Sourced Software.

21 – DISCLOSURE AND CONSENT TO THE USE OF ELECTRONIC COMMUNICATIONS

As part of your relationship with us, we are required by law to give you certain information "in writing." We may also need to obtain your signature to perform certain functions. You can choose to both receive information and to provide necessary signatures related to your relationship with us electronically, instead. In order to do this, we first need your consent to use electronic records and signatures.

By providing your consent to us, you are consenting to the use of electronic records and signatures in connection with your relationship with us, and also confirming that:

- **You have reviewed this Disclosure and Consent,**
- **You agree to receive your account statements from us electronically,**
- **You have the hardware and software described below,**
- **You are able to receive and review electronic records, and**
- **You have an active email account and have provided the correct address to us.**

In this consent, the words "Passport," "we," "us," and "our" means Passport Labs, Inc., its successors, affiliates and assigns. The words "you" and "your" means the person giving consent.

"Communications" means each disclosure, notice, record, document or other information we provide to you, or that you sign or submit or agree to at our request, in connection with your relationship with us and any Service we provide.

"Service" means each and every product or service we offer, provide to you, or that you apply for, own, use, administer or access, either now or in the future.

1. **Scope of your consent. Your consent applies to Communications related to all Services we may make accessible or available, or offer to you, whether through a website, software application, email, messaging services (including text messages), or otherwise. Your consent includes, but is not limited to, all Communications related to parking and transit payment services, your registration and account with us, and the use of the Passport website ("Website") and mobile application ("Mobile App").**
2. **Delivery of Communications.** In our sole discretion, the Communications we provide to you, or that you sign or agree to at our request, may be in electronic form ("Electronic Records"). We may also use **electronic** signatures and obtain them from you as part of our transactions with you. Electronic Records may be delivered to you by (i) posting on the Website, (ii) email to you at the email address you provide to us, (iii) through a mobile application, (iv) accessing an online location that we designate in an e-mail, text message or other electronic notice we send to you at the time the Communication is available, or (v) via text message at the phone number you provide to us, if you agree to do so.

We may always, in our sole discretion, provide you with any Communication in writing or send it to you via the U.S. mail or other means of delivery, even if you have chosen to receive it electronically. We may require any information you provide to us, or any document you sign, to be delivered to us in writing. You should print or download a copy of any Electronic Records for your own records, including this Disclosure and Consent.

1. **Your option to receive paper copies.** If we provide an Electronic Record to you, and you want a paper copy, you may call our End User Support team at (704) 837-8066 or email support@passportinc.com and request a paper version. You may have to pay a fee for the paper copy unless charging a fee is prohibited by applicable law.
2. **You may withdraw your consent at any time; Consequences of withdrawing consent; How to give notice of withdrawal.** You have the right to withdraw your consent at any time. Please be aware, however, that withdrawal of consent may result in the termination of your use of or access to certain Services. To withdraw your consent, contact our End User Support team at (704) 837-8066 or via email at support@passportinc.com. Your withdrawal of consent will become effective after we have had a reasonable opportunity to act upon it.
3. **You must keep your contact information current with us.** You must notify us immediately of any change to the email, telephone, or mailing addresses you provide to us ("Contact Information"). You can make changes to your Contact Information by changing your profile information, calling our End User Support team at (704) 837-8066, or emailing support@passportinc.com.
4. **System Requirements**: In order to view and retain your electronic Communications, you will need:

- Internet access, a Current Version of an internet browser we support;
- A mobile device running a Current Version of the Mobile App;
- A printer or other storage device; and
- An active email address.

You must have a computer or handheld device using a Current Version of an operating system capable of supporting all of the requirements described above. By "Current Version", we mean a version of the software currently supported by its publisher. We reserve the right to discontinue support of a Current Version of software if, in our sole opinion, it suffers from a security flaw or other flaw that makes it unsuitable for our use of electronic Communications. In some cases, you may also need a specific brand or type of device that can support a particular software application, including an application intended for particular mobile or handheld devices. To receive text messages you will need an active telephone number and a device capable of receiving text messages sent to that number.

If we change these hardware or software requirements, and that change creates a material risk that you would not be able to access or retain your electronic Communications, we will notify you of the revised hardware or software requirements, but you will continue to receive electronic Communications until you withdraw your consent.

In the event of a complaint or concern regarding this Agreement or the Platform, or for more information, please contact Company at 704-837-8066 or info@gopassport.com.

Terms

Updated Dec 20, 2020

Acceptance of the Terms of Use

These terms of use are entered into by and between You and LFE, Inc. ("**Company**," "**we**," or "**us**"). The following terms and conditions (collectively, "**Terms of Use**") govern your access to and use of the Honk mobile application (the "**App**"), whether as a guest or a registered user.

Please read the Terms of Use carefully before you start to use the App. **By using the App or by clicking to accept or agree to the Terms of Use when this option is made available to you, you accept and agree to be bound and abide by these Terms of Use and our Privacy Policy, found at honk.me/privacy, incorporated herein by reference.** If you do not want to agree to these Terms of Use or the Privacy Policy, you must not access or use the App.

This App is offered and available to users who are 13 years of age or older. By using this App, you represent and warrant that you meet all of the App's eligibility requirements. If you do not meet all of these requirements, you must not access or use the App.

Changes to the Terms of Use

We may revise and update these Terms of Use from time to time in our sole discretion. All changes are effective immediately when we post them, and apply to all access to and use of the App thereafter.

Your continued use of the App following the posting of revised Terms of Use means that you accept and agree to the changes. You are expected to check this page from time to time so you are aware of any changes, as they are binding on you.

Account Security

If you choose a user name, password, or any other piece of information as part of our security procedures, you must treat that information as confidential, and you must not disclose it to any other person or entity. You also acknowledge that your account is personal to you and agree not to provide any other person with access to this App or portions of it using your user name, password, or other security information. You agree to notify us immediately of any unauthorized access to or use of your user name or password or any other breach of security.

We have the right to disable any user name, password, or other identifier, whether chosen by you or provided by us, at any time in our sole discretion for any or no reason, including if, in our opinion, you have violated any provision of these Terms of Use.

Intellectual Property Rights

The App and its entire contents, features, and functionality (including but not limited to all information, software, text, displays, images, video, and audio, and the design, selection, and arrangement thereof) are owned by the Company and are protected by United States and international intellectual property or proprietary rights laws.

Prohibited Uses

You may use the App only for lawful purposes and in accordance with these Terms of Use. You agree not to use the App:

- In any way that violates any applicable federal, state, local, or international law or regulation.
- For the purpose of exploiting, harming, or attempting to exploit or harm minors in any way by exposing them to inappropriate content, asking for personally identifiable information, or otherwise.

- To send, knowingly receive, upload, download, use, or re-use any material that does not comply with the Content Standards set out in these Terms of Use.
- To transmit, or procure the sending of, any advertising or promotional material, including any "junk mail," "chain letter," "spam," or any other similar solicitation.
- To impersonate or attempt to impersonate the Company, a Company employee, another user, or any other person or entity (including, without limitation, by using email addresses or screen names associated with any of the foregoing).
- To engage in any other conduct that restricts or inhibits anyone's use or enjoyment of the App, or which, as determined by us, may harm the Company or users of the App, or expose them to liability.

Additionally, you agree not to:

- Use the App in any manner that could disable, overburden, damage, or impair the App or interfere with any other party's use of the App, including their ability to engage in real time activities through the App.
- Use any robot, spider, or other automatic device, process, or means to access the App for any purpose, including monitoring or copying any of the material on the App.
- Use any manual process to monitor or copy any of the material on the App, or for any other purpose not expressly authorized in these Terms of Use, without our prior written consent.
- Use any device, software, or routine that interferes with the proper working of the App.
- Introduce any viruses, Trojan horses, worms, logic bombs, or other material that is malicious or technologically harmful.
- Attempt to gain unauthorized access to, interfere with, damage, or disrupt any parts of the App, the server on which the App is stored, or any server, computer, or database connected to the App.
- Attack the App via a denial-of-service attack or a distributed denial-of-service attack.
- Otherwise attempt to interfere with the proper working of the App.

User Contributions

The App contains interactive features ("**Interactive Services**") that allow users to post, submit, publish, display, or transmit to other users or other persons (hereinafter, "**post**")

content or materials (collectively, "**User Contributions**") on or through the App.

All User Contributions must comply with the Content Standards set out in these Terms of Use.

Any User Contribution you post while using the App will be considered non-confidential and non-proprietary.

You understand and acknowledge that you are responsible for any User Contributions you submit or contribute, and you, not the Company, have full responsibility for such content, including its legality, reliability, accuracy, and appropriateness.

We are not responsible or liable to any third party for the content or accuracy of any User Contributions posted by you or any other user of the App.

Monitoring and Enforcement; Termination

We have the right to:

- Remove or refuse to post any User Contributions for any or no reason in our sole discretion.
- Take any action with respect to any User Contribution that we deem necessary or appropriate in our sole discretion, including if we believe that such User Contribution violates the Terms of Use, including the Content Standards, infringes any intellectual property right or other right of any person or entity, threatens the personal safety of users of the App or the public, or could create liability for the Company.
- Disclose your identity or other information about you to any third party who claims that material posted by you violates their rights, including their intellectual property rights or their right to privacy.
- Take appropriate legal action, including without limitation, referral to law enforcement, for any illegal or unauthorized use of the App.
- Terminate or suspend your access to all or part of the App for any or no reason, including without limitation, any violation of these Terms of Use.

We will:

- Investigate reports submitted to us of objectionable content or user within 24 hours of receipt; and
- Remove the user who has been reported to us if we decide (at our sole discretion) that the user has breached the Terms of Use.

Without limiting the foregoing, we have the right to cooperate fully with any law enforcement authorities or court order requesting or directing us to disclose the identity or other information of anyone posting any materials on or through the App. YOU WAIVE AND HOLD HARMLESS THE COMPANY AND ITS AFFILIATES, LICENSEES, AND SERVICE PROVIDERS FROM ANY CLAIMS RESULTING FROM ANY ACTION TAKEN BY ANY OF THE FOREGOING PARTIES DURING, OR TAKEN AS A CONSEQUENCE OF, INVESTIGATIONS BY EITHER SUCH PARTIES OR LAW ENFORCEMENT AUTHORITIES.

However, we cannot review all material before it is posted on the App, and cannot ensure prompt removal of objectionable material after it has been posted. Accordingly, we assume no liability for any action or inaction regarding transmissions, communications, or content provided by any user or third party. We have no liability or responsibility to anyone for performance or nonperformance of the activities described in this section.

Content Standards

These content standards apply to any and all User Contributions and use of Interactive Services. User Contributions must in their entirety comply with all applicable federal, state, local, and international laws and regulations. Without limiting the foregoing, User Contributions must not:

- Contain any material that is defamatory, obscene, indecent, abusive, offensive, harassing, violent, hateful, inflammatory, or otherwise objectionable.
- Infringe any patent, trademark, trade secret, copyright, or other intellectual property or other rights of any other person.
- Violate the legal rights (including the rights of publicity and privacy) of others or contain any material that could give rise to any civil or criminal liability under applicable laws or regulations or that otherwise may be in conflict with these Terms of Use and our Privacy Policy.
- Promote any illegal activity, or advocate, promote, or assist any unlawful act.
- Impersonate any person, or misrepresent your identity or affiliation with any person or organization.

- Give the impression that they emanate from or are endorsed by us or any other person or entity, if this is not the case.

Copyright Infringement

If you believe that any User Contributions violate your copyright, please see our Copyright Policy below for instructions on sending us a notice of copyright infringement. It is the policy of the Company to terminate the user accounts of repeat infringers.

Changes to the App

We may update the content on this App from time to time, but its content is not necessarily complete or up-to-date. Any of the material on the App may be out of date at any given time, and we are under no obligation to update such material.

Disclaimer of Warranties

You understand that we cannot and do not guarantee or warrant that files available for downloading from the internet or the App will be free of viruses or other destructive code. You are responsible for implementing sufficient procedures and checkpoints to satisfy your particular requirements for anti-virus protection and accuracy of data input and output, and for maintaining a means external to our App for any reconstruction of any lost data. TO THE FULLEST EXTENT PROVIDED BY LAW, WE WILL NOT BE LIABLE FOR ANY LOSS OR DAMAGE CAUSED BY A DISTRIBUTED DENIAL-OF-SERVICE ATTACK, VIRUSES, OR OTHER TECHNOLOGICALLY HARMFUL MATERIAL THAT MAY INFECT YOUR COMPUTER EQUIPMENT, COMPUTER PROGRAMS, DATA, OR OTHER PROPRIETARY MATERIAL DUE TO YOUR USE OF THE APP OR ANY SERVICES OR ITEMS OBTAINED THROUGH THE APP OR TO YOUR DOWNLOADING OF ANY MATERIAL POSTED ON IT, OR ON ANY APP LINKED TO IT.

YOUR USE OF THE APP, ITS CONTENT, AND ANY SERVICES OR ITEMS OBTAINED THROUGH THE APP IS AT YOUR OWN RISK. THE APP, ITS CONTENT, AND ANY SERVICES OR ITEMS OBTAINED THROUGH THE APP ARE PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS, WITHOUT ANY WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED. NEITHER THE COMPANY NOR ANY PERSON ASSOCIATED WITH THE COMPANY MAKES ANY WARRANTY OR REPRESENTATION WITH RESPECT

TO THE COMPLETENESS, SECURITY, RELIABILITY, QUALITY, ACCURACY, OR AVAILABILITY OF THE APP. WITHOUT LIMITING THE FOREGOING, NEITHER THE COMPANY NOR ANYONE ASSOCIATED WITH THE COMPANY REPRESENTS OR WARRANTS THAT THE APP, ITS CONTENT, OR ANY SERVICES OR ITEMS OBTAINED THROUGH THE APP WILL BE ACCURATE, RELIABLE, ERROR-FREE, OR UNINTERRUPTED, THAT DEFECTS WILL BE CORRECTED, THAT OUR APP OR THE SERVER THAT MAKES IT AVAILABLE ARE FREE OF VIRUSES OR OTHER HARMFUL COMPONENTS, OR THAT THE APP OR ANY SERVICES OR ITEMS OBTAINED THROUGH THE APP WILL OTHERWISE MEET YOUR NEEDS OR EXPECTATIONS.

TO THE FULLEST EXTENT PROVIDED BY LAW, THE COMPANY HEREBY DISCLAIMS ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, STATUTORY, OR OTHERWISE, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR PARTICULAR PURPOSE.

THE FOREGOING DOES NOT AFFECT ANY WARRANTIES THAT CANNOT BE EXCLUDED OR LIMITED UNDER APPLICABLE LAW.

Limitation on Liability

TO THE FULLEST EXTENT PROVIDED BY LAW, IN NO EVENT WILL THE COMPANY, ITS AFFILIATES, OR THEIR LICENSORS, SERVICE PROVIDERS, EMPLOYEES, AGENTS, OFFICERS, OR DIRECTORS BE LIABLE FOR DAMAGES OF ANY KIND, UNDER ANY LEGAL THEORY, ARISING OUT OF OR IN CONNECTION WITH YOUR USE, OR INABILITY TO USE, THE APP, ANY APPS LINKED TO IT, ANY CONTENT ON THE APP OR SUCH OTHER APPS, INCLUDING ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES, INCLUDING BUT NOT LIMITED TO, PERSONAL INJURY, PAIN AND SUFFERING, EMOTIONAL DISTRESS, LOSS OF REVENUE, LOSS OF PROFITS, LOSS OF BUSINESS OR ANTICIPATED SAVINGS, LOSS OF USE, LOSS OF GOODWILL, LOSS OF DATA, AND WHETHER CAUSED BY TORT (INCLUDING NEGLIGENCE), BREACH OF CONTRACT, OR OTHERWISE, EVEN IF FORESEEABLE.

The limitation of liability set out above does not apply to liability resulting from our gross negligence or willful misconduct.

THE FOREGOING DOES NOT AFFECT ANY LIABILITY THAT CANNOT BE EXCLUDED OR LIMITED UNDER APPLICABLE LAW.

Indemnification

You agree to defend, indemnify, and hold harmless the Company, its affiliates, licensors, and service providers, and its and their respective officers, directors, employees, contractors, agents, licensors, suppliers, successors, and assigns from and against any claims, liabilities, damages, judgments, awards, losses, costs, expenses, or fees (including reasonable attorneys' fees) arising out of or relating to your violation of these Terms of Use or your use of the App, including, but not limited to, your User Contributions, any use of the App's content, services, and products other than as expressly authorized in these Terms of Use, or your use of any information obtained from the App.

Governing Law and Jurisdiction

All matters relating to the App and these Terms of Use, and any dispute or claim arising therefrom or related thereto (in each case, including non-contractual disputes or claims), shall be governed by and construed in accordance with the internal laws of the State of California without giving effect to any choice or conflict of law provision or rule (whether of the State of California or any other jurisdiction).

Any legal suit, action, or proceeding arising out of, or related to, these Terms of Use or the App shall be instituted exclusively in the federal courts of the United States or the courts of the State of California, in each case located in the City of San Francisco, although we retain the right to bring any suit, action, or proceeding against you for breach of these Terms of Use in your country of residence or any other relevant country. You waive any and all objections to the exercise of jurisdiction over you by such courts and to venue in such courts.

Limitation on Time to File Claims

ANY CAUSE OF ACTION OR CLAIM YOU MAY HAVE ARISING OUT OF OR RELATING TO THESE TERMS OF USE OR THE APP MUST BE COMMENCED WITHIN ONE (1) YEAR AFTER THE CAUSE OF ACTION ACCRUES; OTHERWISE, SUCH CAUSE OF ACTION OR CLAIM IS PERMANENTLY BARRED.

Waiver and Severability

No waiver by the Company of any term or condition set out in these Terms of Use shall be deemed a further or continuing waiver of such term or condition or a waiver of any other term or condition, and any failure of the Company to assert a right or provision under these Terms of Use shall not constitute a waiver of such right or provision.

If any provision of these Terms of Use is held by a court or other tribunal of competent jurisdiction to be invalid, illegal, or unenforceable for any reason, such provision shall be eliminated or limited to the minimum extent such that the remaining provisions of the Terms of Use will continue in full force and effect.

Entire Agreement

The Terms of Use and our Privacy Policy constitute the sole and entire agreement between you and LFE, Inc. regarding the App and supersede all prior and contemporaneous understandings, agreements, representations, and warranties, both written and oral, regarding the App.

Your Comments and Concerns

This App is operated by LFE, Inc. 1150 Foothill Blvd # D, La Cañada Flintridge, CA 91011.

All notices of copyright infringement claims should be sent to the copyright agent designated in our Copyright Policy in the manner and by the means set out therein.

All other feedback, comments, requests for technical support, and other communications relating to the App should be directed to: legal@honk.me

Copyright Policy

Reporting Claims of Copyright Infringement

We take claims of copyright infringement seriously. We will respond to notices of alleged copyright infringement that comply with applicable law. If you believe any

materials accessible on or from this App infringe your copyright, you may request removal of those materials (or access to them) from the App by submitting written notification to our copyright agent designated below. In accordance with the Online Copyright Infringement Liability Limitation Act of the Digital Millennium Copyright Act (17 U.S.C. § 512) ("**DMCA**"), the written notice (the "**DMCA Notice**") must include substantially the following:

- Your physical or electronic signature.
- Identification of the copyrighted work you believe to have been infringed or, if the claim involves multiple works on the App, a representative list of such works.
- Identification of the material you believe to be infringing in a sufficiently precise manner to allow us to locate that material.
- Adequate information by which we can contact you (including your name, postal address, telephone number, and, if available, email address).
- A statement that you have a good faith belief that use of the copyrighted material is not authorized by the copyright owner, its agent, or the law.
- A statement that the information in the written notice is accurate.
- A statement, under penalty of perjury, that you are authorized to act on behalf of the copyright owner.

If you fail to comply with all of the requirements of Section 512(c)(3) of the DMCA, your DMCA Notice may not be effective.

Please be aware that if you knowingly materially misrepresent that material or activity on the App is infringing your copyright, you may be held liable for damages (including costs and attorneys' fees) under Section 512(f) of the DMCA.

Please send notifications of copyright infringement to LFE, Inc., Attn: Copyright Agent, 1150 Foothill Blvd # D, La Cañada Flintridge, CA 91011, legal@honk.me

Terms of Use

Choose Your Language

Thanks for using our products and services ("Services")! The Services ar Parkmobile, LLC ("ParkMobile"), located at 1100 Spring Street, NW, Suite Georgia 30309, United States.

By using our Services, you are agreeing to these terms and our priv read them carefully.

We offer a variety of Services so sometimes additional terms may apply. will be available with the relevant Services, and those additional terms wi of your agreement with us, if you use those Services.

Changes to the Terms

We may modify these terms or any additional terms that apply to a Servic reflect changes to the law or changes to our Services. You should look at regularly. We'll post notice of modifications to these terms on this page. V modified additional terms in the applicable Service. Changes will not app will become effective no sooner than fourteen days after they are postec changes addressing new functions for a Service or changes made for le effective immediately. If you do not agree to the modified terms for a Serv discontinue your use of that Service.

Using our Services

You may use our Services only if you can legally form a binding contract v accordance with these terms and all applicable laws. You can't use our S be prohibited by U.S. sanctions. Any use or access by anyone under the a allowed. Using ParkMobile may include downloading software to your ph

We are a technology company. We do not own, operate, or maintain any p
we do not provide parking enforcement services. Parking facilities are op
parties. Parking restrictions (i.e. no parking signs) take precedence over
you receive from us. All applicable parking rules and regulations apply to
of the Services does not excuse you from following the rules.

Your ParkMobile Account

You may need a ParkMobile account in order to use some of our Service
your own ParkMobile account, or your ParkMobile account may be assig
administrator, such as your employer. When you create your ParkMobile
provide us with accurate and complete information. If you are using a Par
assigned to you by an administrator, different or additional terms may ap
administrator may be able to access or disable your account.

Limited License to Use Our Services

Subject to your compliance with these terms, ParkMobile grants you a lir
exclusive, non-sublicensable, revocable, non-transferable license to: (i) a
applications on your personal device solely in connection with your use
(ii) access and use any content, information and related materials that ma
available through the Services, in each case solely for your personal, nor
Any rights not expressly granted herein are reserved by ParkMobile and
licensors.

Text Messaging

Text2Park (Shortcode: 77223)

You can cancel the SMS service at any time. Just text "STOP" to 77223. A
will send you a text message to confirm that you have been unsubscribe
Text2Park program. After this, you will no longer receive text messages r
Text2Park program. If you have opted into our other SMS services (i.e. pa
you may continue to receive text messages originating from those progr

If you experience issues with our Text2Park service, just text “HELP” to 7
contact our customer care center **online** or by calling us at **(877) 727-54**

Ready to Park
Reserve Parki
Solutions for P
More +
Blog
Contact Us
Fleet Sign In

us from you. Message frequency varries. If you have any questions about
data plan, it is best to contact your wireless provider.

If you have any questions regarding privacy, please visit our **privacy poli**

SMS Parking Notifications

By providing your phone number to opt-in to receive parking notifications
receive a text message when your parking session is about to expire, and
after your parking session has ended. Message and data rates may apply
your notification preferences at any time through your account settings.
contact our customer care center **online** or by calling us at **(877) 727-54**

Network Access and Devices

You are responsible for obtaining the data network access necessary to
Your mobile network's data and messaging rates and fees may apply if yo
the Services from your device. You are responsible for acquiring and upd
hardware or devices necessary to access and use the Services and any
guarantee that the Services will function on any particular hardware or de
the Services may be subject to malfunctions and delays inherent in the us
and electronic communications.

Payment

You understand that use of the Services may result in charges to you for
receive ("Charges"). We will receive and/or enable your payment of the ap
for services obtained through your use of the Services. Charges will be in
applicable taxes where required by law. Charges may include other appli
processing fees.

All Charges and payments will be enabled by ParkMobile using the prefe
method designated by you in your account, after which you will receive a
your primary account payment method is determined to be expired, inval
able to be charged, you agree that we may use a secondary payment me
account, if available. Charges paid by you are final and non-refundable, u
determined by ParkMobile.

Ready to Park
Reserve Parki
Solutions for P
More +
Blog
Contact Us
Fleet Sign In

provided that you will be responsible for Charges incurred under your ac
your awareness of such Charges or the amounts thereof. We may from ti
certain users with promotional offers and discounts that may result in diff
charged for the same or similar services or goods obtained through the u
and you agree that such promotional offers and discounts, unless also m
you, shall have no bearing on your use of the Services or the Charges app

In certain cases, with respect to third party providers, Charges you incur
directly to third party providers, and ParkMobile will collect payment of th
you, on the third party provider's behalf as their limited payment collectio
payment of the Charges shall be considered the same as payment made
the third party provider.

Sweepstakes and Other Promotions

In addition to these terms, sweepstakes, contests or other promotions (c
"Promotions") made available through the Services may have specific rul
from these terms. By participating in a Promotion, you will become subje
We urge you to review the rules before you participate in a Promotion. Pr
control over any conflict with these terms.

Intellectual Property

We reserve all of our intellectual property rights in the Services. Tradema
in connection with the Services are the trademarks of their respective ov
and "P" logos and other ParkMobile trademarks, service marks, graphics
our Services are trademarks or registered trademarks of ParkMobile, LL

Security

We care about the security of our users. While we work to protect the se
content and account, we can't guarantee that unauthorized third parties
defeat our security measures. We ask that you keep your password secu
immediately of any unauthorized use of your account.

Modifying and Terminating our Services

Ready to Park
Reserve Parki
Solutions for P
More +
Blog
Contact Us
Fleet Sign In

You can stop using our Services at any time, although we'll be sorry to se terminate or suspend your right to access or use our Services for any rea notice. ParkMobile may also stop providing Services to you or add or cre our Services at any time.

Third-party Links

Our Services may contain links to other websites and resources provide that are not owned or controlled by us. We have no control over the conte websites or resources. If you access any third-party content from our Se your own risk and subject to the terms and conditions of use for such thir

Disclaimer of Warranties

Our Services are provided on an "as is" basis without warranty of any kinc or implied, statutory or otherwise. We specifically disclaim any and all wa merchantability, non-infringement, and fitness for a particular purpose.

Limitation of Liability

TO THE MAXIMUM EXTENT ALLOWED BY LAW, IN NO EVENT WILL T LIABILITY OF PARKMOBILE AND ITS SUBSIDIARIES AND AFFILIATES RESPECTIVE LICENSORS, SERVICE PROVIDERS, EMPLOYEES, AGE MEMBERS, MANAGERS AND DIRECTORS, TO ANY PARTY (REGARD FORM OF ACTION, WHETHER IN CONTRACT, TORT, OR OTHERWIS AMOUNT YOU HAVE PAID TO PARKMOBILE TO USE THE SERVICES

Business Uses of Our Services

If you want to use ParkMobile for commercial purposes, you must create account and agree to our Business Terms of Service. If you do open an a company, organization, or other entity, then "you" includes you and that e promise that you are authorized to grant all permissions and licenses prc terms and bind the entity to these terms, and that you agree to these terr behalf.

General Terms

Ready to Park

Reserve Parki

Solutions for F

More +

Blog

Contact Us

Fleet Sign In

These terms control the relationship between ParkMobile and you. They
third-party beneficiary rights.

If you do not comply with these terms, and we don't take action right awa
that we are giving up any rights that we may have (such as taking action ir

If it turns out that a particular term is not enforceable, this will not affect ar

The laws of the State of Georgia, U.S.A., excluding Georgia's conflict of la
to any disputes arising out of or relating to these terms or the Services. A
of or relating to these terms or the Services will be litigated exclusively in
courts of Fulton County, Georgia, USA, and you and ParkMobile consent
jurisdiction in those courts.

Terms and Conditions

PayByPhone offers Services which allow you to pay for parking in cities around the world. The following terms and conditions govern your Account and use of Services with PayByPhone.

Your contract and Account may be with PayByPhone Technologies Inc. or one of its subsidiaries. The applicable contract party depends on the country from which you open your Account and in which you conduct your Parking Sessions. The contract party is listed below for each of the countries in which the PayByPhone service is available:

Canada	PayByPhone Technologies Inc.
United States	PayByPhone US Inc.
United Kingdom	PayByPhone Limited
France, Monaco, Netherlands, Belgium	PayByPhone SAS
Germany	sunhill technologies GmbH
Switzerland	PayByPhone Suisse AG
Italy	PayByPhone Italia S.r.l.

Collectively, all of these entities are referred to here as “PayByPhone”.

If you use the Service in a country other than the one from which you opened your Account, you will also have a contract, with respect to your Parking Sessions in that country only, with the PayByPhone entity listed above for that country.

At some United States locations, the Service is offered by PayByPhone Technologies Inc. and Parking Sessions at those locations will be subject to your contract with that party.

At some Switzerland locations, the Service is offered by PayByPhone SAS and Parking Sessions at those locations will be subject to your contract with that party.

These Terms and Conditions explain our mutual rights and obligations with regards to the Services. Please read these terms and conditions carefully and keep a copy for future reference.

By creating your Account, accessing, browsing, viewing or otherwise using your Account or the Services, you agree to be legally bound by these Terms and Conditions, the Privacy Policy, the Cookies Policy, the Legal Notice, as well as applicable laws and regulations.

If you do not agree with these Terms and Conditions or the Privacy Policy, please refrain from creating an Account or using the Services.

If you have any questions about the information below, please contact your Customer Support Center listed at the end of this page.

Table of Contents

1. Terms and conditions for PayByPhone's services

These Terms and Conditions govern your use of the Services (including the App and your Account) and are applicable to your use of the App and Services for every Transaction.

This is not an agreement between you and any Transaction Entity or Facilities Operator, this is an agreement between you and PayByPhone, even if you access certain parts of the Services through a third-party website or app.

Our Services are not intended for people under 16. If you become aware that a child is using our Services, please contact the relevant Data Protection Officer listed in Section 15 of the Privacy Policy, and we will take steps to remove and terminate the account as necessary.

In this agreement, the following terms have the meanings indicated below:

- **Account** - The PayByPhone parking service account opened by you in the App, on the Site or by calling our Customer Support Centers.

- **ANPR** – The automatic number plate recognition feature which (1) identifies an opted-in vehicle, prior to payment, as authorized to park at the participating parking facilities and allows access to the parking facilities without having to perform any action normally required to remove a barrier to entry and (2) automatically records the time of entry and exit from the participating parking facility, calculates the length of stay and the cost of the Parking Session for the purposes of initiating payment.
- **App** - The PayByPhone mobile parking payment application and other applications that we may develop.
- **Autopass** – The service from PayByPhone that you opt your vehicle or vehicles in using the App, the Site or our Customer Support Center which allows you to automatically pay for parking at participating parking facility operators that support ANPR.
- **Facilities Operator** - The operator of a parking facility offering the option to pay for parking with the PayByPhone service.
- **Intellectual Property** - Marks, inventions, techniques, methods, works of authorship, know-how, publicity rights, trade secrets, proprietary rights, and all other intellectual property rights related thereto.
- **Payment Information** - Information of any type necessary to process payments by credit cards, debit cards, digital wallets, in-app and web purchases and any other payment method accepted by PayByPhone now or in the future in connection with any Transaction.
- **Parking Penalties** - Parking fines, violation notices, tickets, citations, or penalties; your vehicle being wheel booted, your car being towed, or impounded; and other enforcement of vehicle parking requirements, Forfait Post-Stationnement.
- **Parking Session** - The parking service you obtain from a Facilities Operator within the Transaction. Details of a parking session can include location, license plate, start parking session time, end parking session time and are usually linked to a payment.
- **Services** - All services offered by PayByPhone, including those that allow you to pay for a Parking Session at participating parking clients, including Autopass, pursuant to the terms and conditions of this agreement, such as using our App, Sites, Application Programming Interfaces, backend technologies, products, services, content, features, functions, applications, IVR System, PayByPhone Portal, PayByPhone Business Portal, and any future updates, changes or additions thereto.
- **Site** - All PayByPhone operated websites including https://www.paybyphone.com, https://www.paybyphone.fr, https://www.paybyphone.co.uk, https://www.paybyphone.ch, https://paybyphone-parken.de/en and https://www.pbp.it/, as well as any successors to such sites.
- **Terms and Conditions** - These Terms and Conditions which are accepted and agreed to by you when you open an Account or use the Services, and which govern your use of the App and Services.
- **Transactions** - Any time you start, pay for, complete, or make a Parking Session transaction using our App or Services.
- **Transaction Entity** - The various payment processing companies that help process your Transactions.

2. Account information

You can open your Account by downloading and installing the App; on the Site; or by contacting the appropriate Customer Support Center. You may change your Account profile at any time, but you agree to provide us with your valid registration information, including your contact details. You may not impersonate others or misrepresent your identity to us.

You are responsible for ensuring that your Account information is accurate and current at all times. You further agree to comply with all state or local restrictions that may be applicable to your registration with us. Your Account will be valid until you or PayByPhone cancel it in accordance with these Terms and Conditions, for example, if your Account contains any untruthful information.

You are solely responsible for use of your Account and you agree to notify us immediately in the event of any unauthorized use.

3. License and access to services

Solely for use in connection with the Services, PayByPhone grants you a limited, nontransferable, nonexclusive, revocable license to access the Services and make personal use of the Site and Service. This license does not include any resale or commercial use of PayByPhone's Service; any collection and use of any information, descriptions, or prices; any derivative use of the Site or its contents; any downloading or copying of account information for the benefit of others; or any use of data mining, robots, or similar data gathering and extraction tools. All materials and information related to PayByPhone may not be reproduced, duplicated, copied, sold, resold, visited, or otherwise exploited for any commercial purpose without the express written consent of PayByPhone. Any unauthorized use terminates the permission or license granted by PayByPhone.

You acknowledge and agree that the license to use the Services is conditioned on the following restrictions:

- You shall not share with or assign, copy (except as expressly set forth herein), sublicense, transfer, lease, rent, sell, distribute, or otherwise provide to any third party (i) your license; (ii) the App; (iii) any use of the Services; or (iv) your rights under these Terms and Conditions.
- You shall not (i) modify, adapt, translate, copy, duplicate, disassemble, decompile, reverse assemble, reverse compile, or reverse engineer, or take similar action with respect to the App or Services or any component thereof for any purpose, or (ii) attempt to discover the underlying source code or algorithms of the App or Services (unless enforcement of this restriction is prohibited by applicable law and then, only to the extent specifically permitted by applicable law, and then only upon providing us with reasonable advance written notice and opportunity to respond).
- You shall not engage in competitive analysis, benchmarking, use, evaluation or viewing of the Services or create any derivatives based upon the App or Services.
- You shall not permit any party, whether acting directly or on your behalf, to breach or violate any of these restrictions.
- You shall not breach any of these Terms and Conditions.

4. Using your account

Purpose

You can use the Account to pay for parking at any parking facility that offers the option to pay with the PayByPhone service and, if the option is available in your region, pay for parking permits and Parking Penalties. You can access your Transactions and review your recent account history on our Site, the App or by calling a Customer Support Center.

Use of Account, Password, and your Cell Phone

When you open an Account, you will be asked to enter a confidential password to securely access your Account. You will also provide us with the number of the phone you will use to access the Account. The Account and password are for your use and protection. You agree:

- Not to disclose the password and not to record it on your phone or otherwise make it available to anyone else.
- To use the Account, the password, and your phone as instructed.
- To promptly notify us of any loss, unauthorized use, or theft of your Account or password.
- To be liable for any transactions made by a person you authorize or permit to use your Account and/or password. If you permit someone else to use the Account, we and the Facilities Operator will treat this as if you have authorized this person to use the Account and you will be responsible for any transactions initiated by such person with the Account.

5. Pricing, payment and refunds

Pricing

You agree that the fees and service charges included in the Transaction are confirmed before you start parking apply to the Account and may be charged to the Account. You authorize us to initiate any such charges to the Account.

You are subject to any applicable terms, conditions, restrictions, and other requirements of any payment provider related to any Payment Method and we have no liability for any transaction fees, insufficient fund charges, or any other fee or charge that is assessed by a payment provider in connection with your use of such payment provider for Transactions.

You understand that parking rates vary as a result of parameters set by the Transaction Entity and Facilities Operator, such as parking location, time of day, day of the week, special events, and that these variances are beyond our control and may not be reflected in the App or Services in a timely manner. We pass all parking fees and charges through to you and we are not responsible for any parking rate variances, parking rate changes or for any differences between the parking rates reflected in the App or Service and the parking rates assessed by the Transaction Entity or Facilities Operator at the time of the Parking Session. You are solely responsible for Parking Penalties and for determining the parking rates applicable to your Parking Session before commencing a Transaction.

You are also solely responsible for all fees or charges you incur in connection with your use of your mobile device to access the App or Services, including but not limited to, data usage, texting, data overages, per-minute charges, roaming, and other telecom or access charges and you acknowledge that such fees or charges may apply and that you are solely responsible for such charges and fees.

A chargeback fee ($15.00, €15.00 or a similar amount in another currency) may be assessed if an attempt to charge your Account is rejected for insufficient funds available on your selected Payment Method, for cancellation of your Payment Method or otherwise.

Payment

You agree to pay the parking fee together with all other fees, charges, or assessments related to Transactions. Payments shall be in the currency of the country where the parking facility is located and will be made to PayByPhone or the Facilities Operator, depending on the location of the parking facility. The amount of the Transaction includes the price specified by the Facilities Operator on the date of service (as posted at the parking facility or configured in the PayByPhone rates system), the service charge for the PayByPhone service, and any taxes that apply and will be charged to the Payment Method selected for the Account.

Refunds

We will make every attempt to deliver a high level of service at all times. If you think there has been a billing or accounting error, please contact the appropriate Customer Support Center listed at the end of this page. If the payment to which the error relates was made to the Facilities Operator, we will connect you to the Facilities Operator. If you are entitled to a refund for any reason for services obtained with the Account, you agree to accept credits to the Payment Method selected on the Account in place of cash. PayByPhone and the Facilities Operators will not provide cash refunds.

If you have any questions about a refund or other similar issue, please contact the appropriate Customer Support Center.

6. Verification of transactions

Details of your Transactions will be available in real time on your online statement in your Account, the App or on our Site. You agree that we may provide you periodic statements and any other notices related to our Services electronically via your Account, the App or our Site. Statements provided electronically will describe each Transaction during the statement period. Your statement will be available to you in electronic format for viewing and printing online on our App and Site. You may review your recent Transaction history in your Account at any time, currently set at one year’s worth of Transactions.

7. Failure to complete transactions

You understand that using the Services does not guarantee you a parking space and you only activate the Services after you have found an available and valid parking space.

You understand that you are solely responsible for ensuring that you have properly started the Parking Session for the appropriate parking location before you leave your vehicle unattended.

You acknowledge and agree that you are solely responsible for correctly entering the relevant information in relation to your parking Transactions, including (i) parking location number for the relevant parking space, (ii) license plate number of the vehicle you are parking, and (iii) information about the Payment Method for the Transaction.

As part of the Services, PayByPhone may send you reminders, alerts, or critical notifications via push notification, text message or email. You acknowledge and agree that the reception of any such message is not 100% guaranteed and that you are responsible for the timely activation or deactivation of a Parking Session where permitted. You acknowledge that you may not receive these notifications due to the operation, coverage, and services of your mobile network provider and/or Internet service provider or for other reasons and agree that you remain responsible for timely activating, extending or deactivating a Parking Session. PayByPhone shall have no liability for any damages and costs you incur from not receiving notifications on time or at all.

We and the Facilities Operators accept no liability to complete any transaction which cannot be cleared by our payment processors, whether because there are insufficient funds available on your Payment Method or otherwise.

Neither we nor any of the Facilities Operators will be liable to you for any failure to accept or honor the Account.

8. PayByPhone is a mobility parking payment solution company

PayByPhone provides a service to enable your payment for parking at certain facilities. PayByPhone does not own, operate or maintain parking facilities and is NOT RESPONSIBLE FOR ANY SUCH FACILITIES OR EVENTS THAT OCCUR AT SUCH FACILITIES. Parking facilities are operated by companies or governmental bodies with which PayByPhone has contractual relationships, but PayByPhone is not responsible for actions taken by such companies.

You are responsible for complying with all advertised parking restrictions, including physical signs prohibiting parking in a certain area, which shall take precedence over any information that you receive from PayByPhone. PayByPhone will not be responsible for any incorrect or conflicting parking restrictions advertised on signage.

9. Permits and Autopass

We provide some consumers with the opportunity to purchase permits from Facilities Operators and partners ("Permit Issuers"). A permit serves as the official confirmation of your purchase of an item offered for sale by Permit Issuers.

Permit Issuers, not PayByPhone, determine the price and availability of those permits. The Permit Issuers have policies that sometimes prohibit us from issuing permits or performing exchanges or refunds after the purchase of a permit has been made. You understand that if you purchase a permit through PayByPhone, you are nevertheless subject to the rules, policies, and terms of the relevant Permit Issuer.

We provide some consumers with the optional Autopass service, which is available in some countries and provides an ability to automatically pay for parking at the participating parking facilities. You understand that the use of the Autopass service remains subject to the rules, policies, and terms of the relevant Facilities Operator.

10. Disclaimer of service level guarantees

Note that the Services are only available in selected locations and may not be available at all times at all locations. While we will endeavor to provide the best possible service, there are limitations to cellular and payment technologies which may cause interruptions in service. Please note that WE PROVIDE NO SERVICE LEVEL GUARANTEES WHATSOEVER concerning the Service.

Unless the law provides otherwise, you waive and release us from any obligations that could arise due to defenses, rights and claims you have or may have against any third party on account of the use of the Account.

11. Warranties, indemnifications and limits of liability

Disclaimer about Warranties

You understand that the Services are provided on "as is" and "as available" basis. PayByPhone makes no representations or warranties of any kind, express or implied, as to the operation of this Service or the information, content, materials, or products included on our App or Site. You expressly agree that your use of this Site and our Service is at your sole risk.

You also understand and agree that any data, content, or information downloaded or otherwise obtained through your use of the App, Site or Services, including viruses, are obtained at your own discretion and risk and that you will be solely responsible for any damage to your computer system or loss of data that may result from such download.

The "near me" locations service is provided to users as a reference only. Users should always check PayByPhone and Facilities Operator signage for actual location number prior to finalizing a Transaction. PayByPhone accepts no responsibility for Parking Sessions booked using an incorrect location number.

PayByPhone does not own, control or operate parking facilities and does not warrant anything with respect to such facilities. PayByPhone will not be liable for any damages of any kind arising from or related to any parking facility or its operation, including, but not limited to direct, indirect, incidental, punitive, and consequential damages arising from damage to your vehicle, loss of your vehicle, or loss of articles left in your vehicle or for any personal injury in any circumstances.

PayByPhone is also not responsible for any Parking Penalties you incur or receive, even if the Services were used in connection with a Transaction. You are solely responsible for resolving with the relevant authorities and Facilities Operators any issues that you may have regarding Parking Penalties. We do not enforce any parking restrictions and have no ability to control the actions of third parties who enforce parking restrictions or assess parking penalties.

Indemnification

You agree to indemnify, hold harmless and defend PayByPhone with respect to any claim, demand, cause of action, debt, liability, damages, costs or expenses, including reasonable attorney's fees and expenses of PayByPhone's selected attorneys, arising from any third party claim against PayByPhone relating to (i) your violation of law; (ii) your infringement of any Intellectual Property or similar proprietary rights of any person or entity; (iii) any noncompliance with or violation of your License; (iv) your improper or illegal use of the App or Services; (v) any act or omission or willful misconduct of yours; (vi) any breach of any of your representations, warranties, or covenants made herein; and (vii) any failure by you to comply with these Terms and Conditions.

Limitation of Liability

By using the App or Services, you hereby release, remise and forever discharge and give up any and all claims which you may have against PayByPhone, which now or hereafter arise from, relate to or are connected with the use of the App, Site or Services or any third party's use of the App, Site or Service. You further waive, release and give up any and all claims and defenses arising from or relating to any act, event or omission. This includes, without limitation, any claim which could be asserted now or in the future under (i) common or civil law; (ii) any PayByPhone policies, practices, or procedures; and/or (iii) any federal, state, provincial, and/or local statutes or regulations.

To the fullest extent permitted by applicable law, PayByPhone disclaims all warranties, express or implied, including, but not limited to, implied warranties of merchantability and fitness for a particular purpose. PayByPhone does not warrant that our App, Site, its servers, or e-mail, SMS sent from PayByPhone are free of viruses or other harmful components. PayByPhone will not be liable for any damages of any kind arising from the use of our Service, including, but not limited to direct, indirect, incidental, punitive, and consequential damages.

Certain laws do not allow limitations on implied warranties or the exclusion or limitation of certain damages. If these laws apply to you, some or all of the above disclaimers, exclusions, or limitations may not apply to you, and you may have additional rights.

12. Loss, theft or unauthorized use

You are responsible for all authorized uses of your Account. Applicable law may protect you from liability for unauthorized purchases. You understand that your Account is not a credit account and is not protected by laws covering credit accounts.

Tell us AT ONCE if you believe that your Account has been used by an unauthorized person. Telephoning us is the best way to KEEP YOUR POSSIBLE LOSSES DOWN. **If you believe that your phone has been stolen, or that someone has transferred or improperly charged the Account without your permission, contact the appropriate Customer Support Center listed at the end of this page. If you fail to notify us promptly and you are grossly negligent or fraudulent in the handling of the Account, you could incur additional charges.**

If your phone or Payment Method has been reported lost, stolen or otherwise tampered with, we may close the Account to keep your and our losses down.

13. Notice containing information about your right to dispute errors

In case of errors or questions about Transactions on your Account, contact the appropriate Customer Support Center listed at the end of these Terms and Conditions as soon as possible, including if you think the statement or receipt is wrong or if you need more information about a Transaction listed on the statement or receipt. Under most circumstances, we will connect you to the Facilities Operator whose charges resulted in the error or whose Transaction resulted in questions. Disputes involving Facilities Operators will be resolved pursuant to their procedures.

Where the disputed payment was charged by us (rather than a Facilities Operator), you must contact us no later than 30 days after the transaction in question has been made available to you on the online statement.

The following information must be contained in that notice:

- Your name, username and phone number or email address used for the Account.
- Description of the error or the transaction you are unsure about and an explanation as clearly as possible of why you believe it is an error or why you need more information.
- The amount in local currency of the suspected error.

If you tell us verbally, we may require that you send us your complaint or question in writing within 10 business days. Generally, we will tell you the results of our investigation within 10 business days after we hear from you and will promptly correct any error. If we need more time, however, we may take up to 45 calendar days to investigate your complaint or question.

If we decide there was no error, we will send you a written explanation within three business days after we finish our investigation. You may ask for copies of documents that we used in our investigation.

14. Dispute resolution and confidential arbitration

Any dispute relating in any way to the services offered by PayByPhone not resolved in accordance with the preceding Section 13 shall be submitted to confidential arbitration in Vancouver, British Columbia, except that, to the extent you have in any manner violated or threatened to violate PayByPhone's intellectual property rights, PayByPhone may seek injunctive

or other appropriate relief in any Provincial or Federal court in the Province of British Columbia, and you consent to exclusive jurisdiction and venue in such courts. Arbitration under this agreement shall be conducted under the rules then prevailing of the Canadian Arbitration Association conducted by a single arbitrator. The arbitrator's award shall be binding and may be entered as a judgment in any court of competent jurisdiction. To the fullest extent permitted by applicable law, no arbitration under this Agreement shall be joined to an arbitration involving any other party subject to this Agreement, whether through class arbitration proceedings or otherwise.

15. Disclosure of account information to third parties

From time to time, subject to any applicable privacy laws or other laws or regulations, we may provide information about you and the Account, notably:

- To our affiliates and to parking and payment companies with whom we have relationships.
- In response to any subpoena, summons, court or administrative order, or other legal process which we believe requires our compliance.
- In connection with collection of indebtedness or to report losses incurred by us.
- In compliance with any agreement between us and a professional, regulatory or disciplinary body.
- In connection with potential commercial transactions or reorganizations.
- To carefully selected service providers and merchant partners who help us meet your needs by providing or offering our services.
- Or as otherwise provided for in the present Terms and Conditions and **Privacy Policy**

For more on how your information is used, please read our Privacy Policy.

16. Credit or information inquiries

You authorize us to make such credit, employment and investigative inquiries, as we deem appropriate, in connection with the issuance and use of the Account. We can furnish information concerning the Account or credit file to consumer reporting agencies and others who may properly receive that information.

17. Business days

Our business days are all days except Saturdays, Sundays, and statutory holidays.

18. Use of cell phones while driving can be dangerous

Please note that operating a cell phone or any other device while driving can be dangerous and we advise you not to use our Service while operating a vehicle. You agree to indemnify and hold PayByPhone harmless from any or all liability whatsoever for any harm, loss or injury related to use of this Service or the Account while operating any kind of vehicle.

19. Cancellation of your account

You may choose to cancel this agreement by closing your Account on our Site or App, by by contacting the appropriate Customer Support Centre listed at the end of these Terms and Conditions. The termination of this agreement will not affect any of our rights or your obligations arising under this agreement prior to termination and, in accordance with the Privacy Policy, your Account will remain our property at all times.

We may cancel or limit your right to use your Account at any time in the event of the following:

- Reports of unauthorized or unusual credit card use associated with your Account including, but not limited to, notice by the card issuing bank.
- Reports of unauthorized or unusual parking use associated with your Account.
- Abuse by you of the chargeback process provided by your issuing bank.
- Excessive levels of disputes or chargebacks.
- Breach of any term of these Terms and Conditions.
- Where the cardholder name on the payment card associated with the Account does not match the name on the Account unless your Account is linked to a business payment method.
- We are unable to verify or authenticate any information that you provide.
- We believe that activity on your Account poses a significant credit or fraud risk to us.

Our ability to suspend, limit or close your Account does not limit or exclude other remedies we may have if you are otherwise in breach of this Agreement.

20. Applicable law

By opening the Account, you agree that the laws of the jurisdiction in which the PayByPhone with whom you have a contract and Account is domiciled excluding the application of any conflict of laws principles and/or rules. In the case of PayByPhone Technologies Inc. the relevant jurisdiction is the Province of British Columbia, Canada (subject to the provisions of the Consumer Protection Act applicable to residents of Quebec), in the case of PayByPhone US Inc. – the State of Delaware, United States, in the case of PayByPhone Limited – United Kingdom, in the case of PayByPhone SAS – France, in the case of PayByPhone Suisse AG – Switzerland, in the case of PayByPhone Italia S.r.l. – Italy, and in the case of sunhill technologies GmbH – Germany. Notwithstanding the above, you agree that it shall be nevertheless permissible for PayByPhone to apply for equitable relief in any jurisdiction. You also agree to comply with all local laws, rules and regulations, including but not limited to those applicable to online conduct and acceptable Internet content.

21. Intellectual property

All Intellectual Property in the App, the Site and Services is the sole property of PayByPhone and our affiliates or other representatives (as applicable) together with any goodwill, derivatives, new versions, enhancements, updates, changes, etc. of our Intellectual Property, even if wholly or partially based upon your ideas, comments, suggestion, questions, requests, and the like.

Other than as expressly set forth herein, PayByPhone does not grant to you any express or implied ownership or other rights to any Intellectual Property and all such rights are retained by PayByPhone. You are liable for any and all damages of every kind resulting from any infringement by you of our Intellectual Property rights.

Any communications, including, without limitation, e-mails, pictures, audio clips, videos, graphics and/or other material sent directly, or by carbon copy or otherwise from you to PayByPhone or any of our officers, managers, employees, representatives, attorneys, or agents and any postings to the Sites shall become PayByPhone's property upon the transmission of the same. You grant the perpetual and irrevocable right to us to both publicly or non-publicly utilize the same, including the identifying information contained therein, in any manner whatsoever, at no charge.

PayByPhone and other marks indicated on our App and Site are registered trademarks of PayByPhone Limited or our affiliates in Canada, the United States, and other countries. Other PayByPhone graphics, logos, page headers, button icons, scripts, and service names are trademarks or trade dress of PayByPhone Technologies Inc. or our affiliates. PayByPhone’s trademarks and trade dress may not be used in connection with any product or service that is not PayByPhone’s, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits PayByPhone. All other trademarks not owned by PayByPhone or our affiliates that appear on our Site are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by PayByPhone or our affiliates.

22. Miscellaneous

You may not assign, transfer, or sublicense this agreement without PayByPhone’s express written consent. We may transfer our rights under this agreement at any time.

Use of the Account is subject to all applicable rules and customs of any payment processor, clearinghouse, or other association involved in Transactions.

We do not give up our rights by delaying or failing to exercise them at any time.

If any term of this agreement is found by a court to be illegal or not enforceable, all other terms will still be in effect.

If we take legal action against you because of your breach of the terms of this agreement, you must pay reasonable attorney’s fees and other costs of the proceedings. Your responsibility for fees and costs shall in no event exceed the maximum allowed by law.

When you download the App from your device, you may be subject to licenses and/or terms of use established by that mobile device, original equipment manufacturer (OEM), or vehicle manufacturer for your general use of that device and applications downloaded from it. These Terms and Conditions are in addition to the terms of those of the mobile device, OEM, or vehicle manufacturer, as the case may be.

You acknowledge and agree that these Terms, the Privacy Policy, the Legal Notice, and the Cookies Policy, and, if applicable to you, any stored credential agreements and additional terms governing optional Services, constitute the entire agreement of the parties hereto relating to the subject matter hereof, and any prior agreements, understandings, representations and commitments concerning such subject matter, whether oral or written, are hereby superseded and terminated in their entirety and are of no further force or effect.

Some pages on our Sites include links to third party websites. These third party sites are governed by their own privacy statements, and we are not responsible for their operations, including but not limited to their information practices. You should review the privacy statement of those third party sites before providing them with any personally identifiable information.

We may at any time change or repeal these Terms and Conditions, the Privacy Policy, Legal Notice, Cookies Policy or any portion of the Services at any time. You will be notified of any change in the manner provided by applicable law prior to the effective date of the change, including either by email or by posting such update on our Sites or App. All such amendments, updates, modifications, replacements, versions, or revisions are effective immediately upon posting on our Site or App. You specifically agree to accept such notice of change by email sent to the last electronic mail address you have provided to us. However, if the change is made for security purposes, we can implement such change without prior notice. Should you decide that you no longer agree to accept changes or notices electronically, we may cancel or suspend this agreement, or any features or services of the Account described herein at any time. All references in these Terms and Conditions to the Privacy Policy, the Legal Notice, and any other Services matters are references to the same as they are amended, updated, modified, replaced, or revised.

If at any time you would like to contact us with your views about our privacy practices, or with any enquiry relating to your personal information, you can do so by contacting the relevant Data Protection Officer listed in Section 15 of the Privacy Policy.

23. Customer Support Centers

The contact information for our Customer Support Centers is listed below. You can also visit our Customer Support page for any questions, concerns, and inquiries you may have at: https://support.paybyphone.com/hc/en-us/requests/new?ticket_form_id=399967

Location	Contact	Address
USA and Canada	support@paybyphone.com	Suite 403 1168 Hamilton Street Vancouver, BC V6B 2S2 Canada
UK	uksupport@paybyphone.com	Bishops Court 17A The Broadway Old Hatfield AL9 5HZ
The Netherlands	support-nl@paybyphone.com	Saturnus 1, 3824 ME Amersfoort Nederland
France, Monaco, and Switzerland	support@paybyphone.fr	62bis Avenue André Morizet 92100 Boulogne-Billancourt
Belgium	support@paybyphone.be	Saturnus 1, 3824 ME

		Amersfoort Nederland
Germany	+49 9131 – 625 99 25 https://paybyphone-parken.de/support	

PayByPhone is owned by Volkswagen Finance Overseas B.V.

Effective Date: 2022-01-01

paybyphone

PayByPhone is owned by Volkswagen Financial Services AG

Change region

Support and contact

- Help Center
- Contact
- Send us feedback
- Cookies settings

Follow us

-
-
-

About PayByPhone

- About us
- Code of Conduct
- Community Blog
- Contact us
- Leadership Team

- Careers
- DEI at PayByPhone

Get the app

- Parking operators
- Terms & Conditions
- Privacy
- Whistleblowing

North America

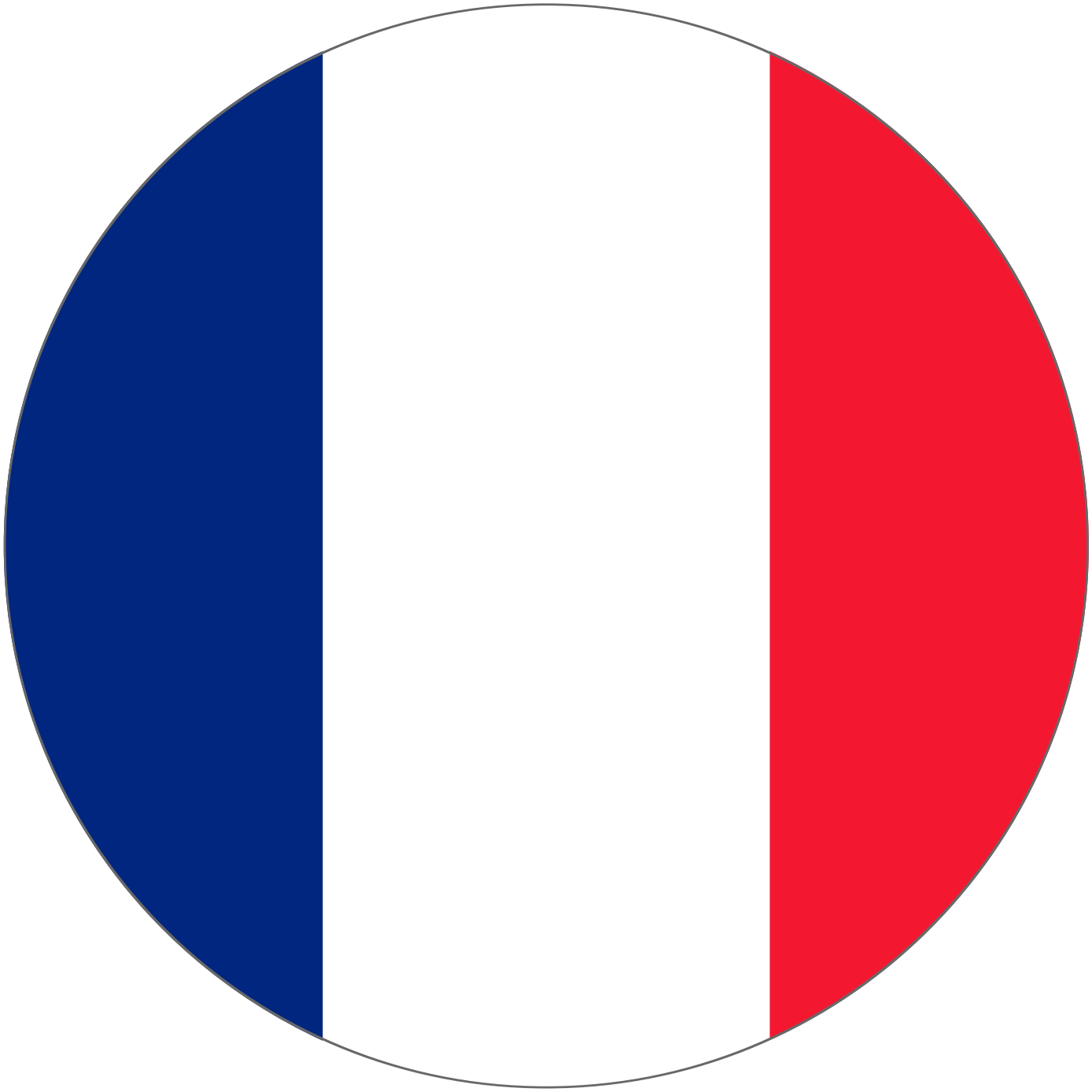
Select your region

- United States

- Canada (EN)

- Canada (FR)

- United Kingdom



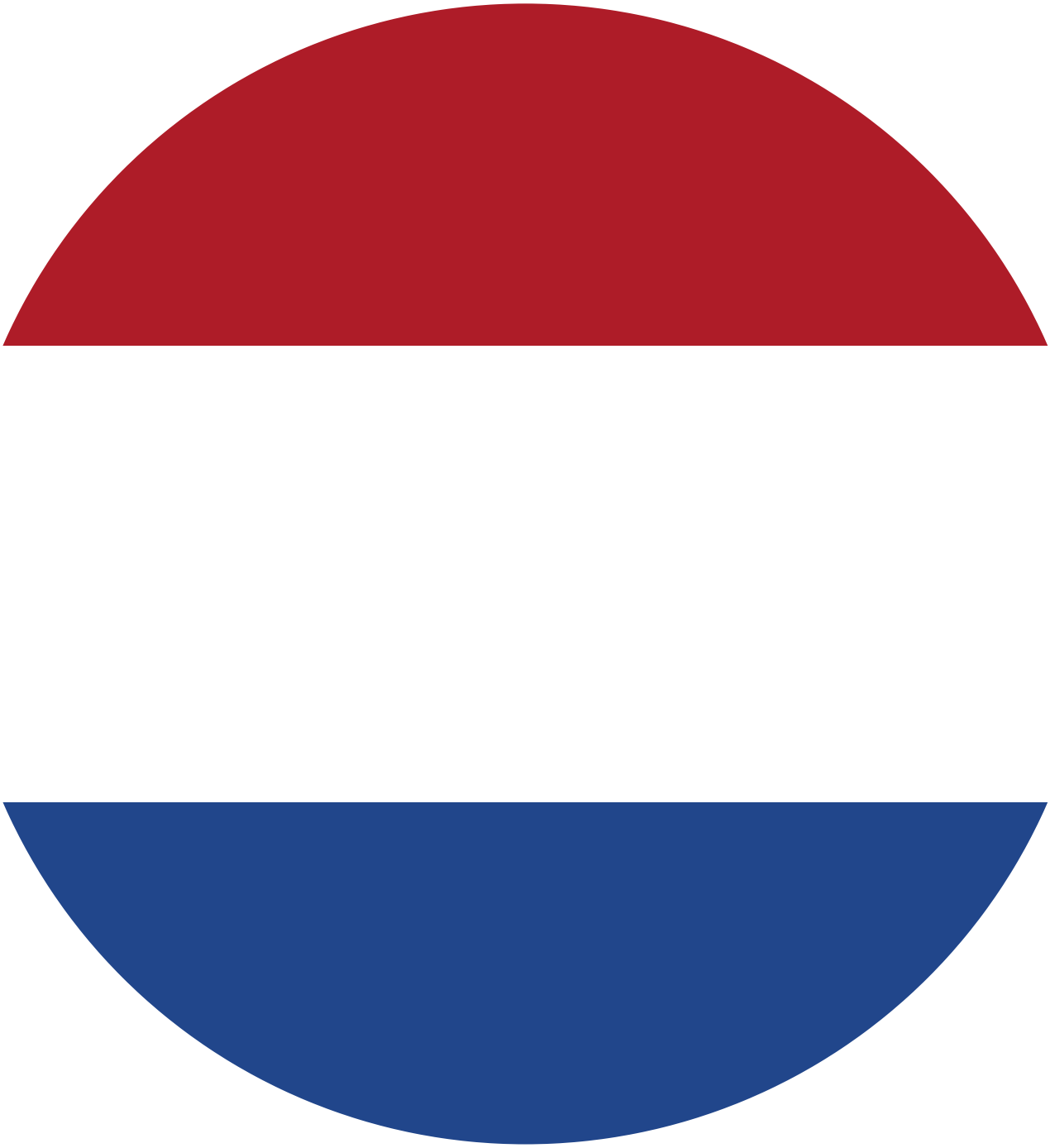
- France

- Belgique

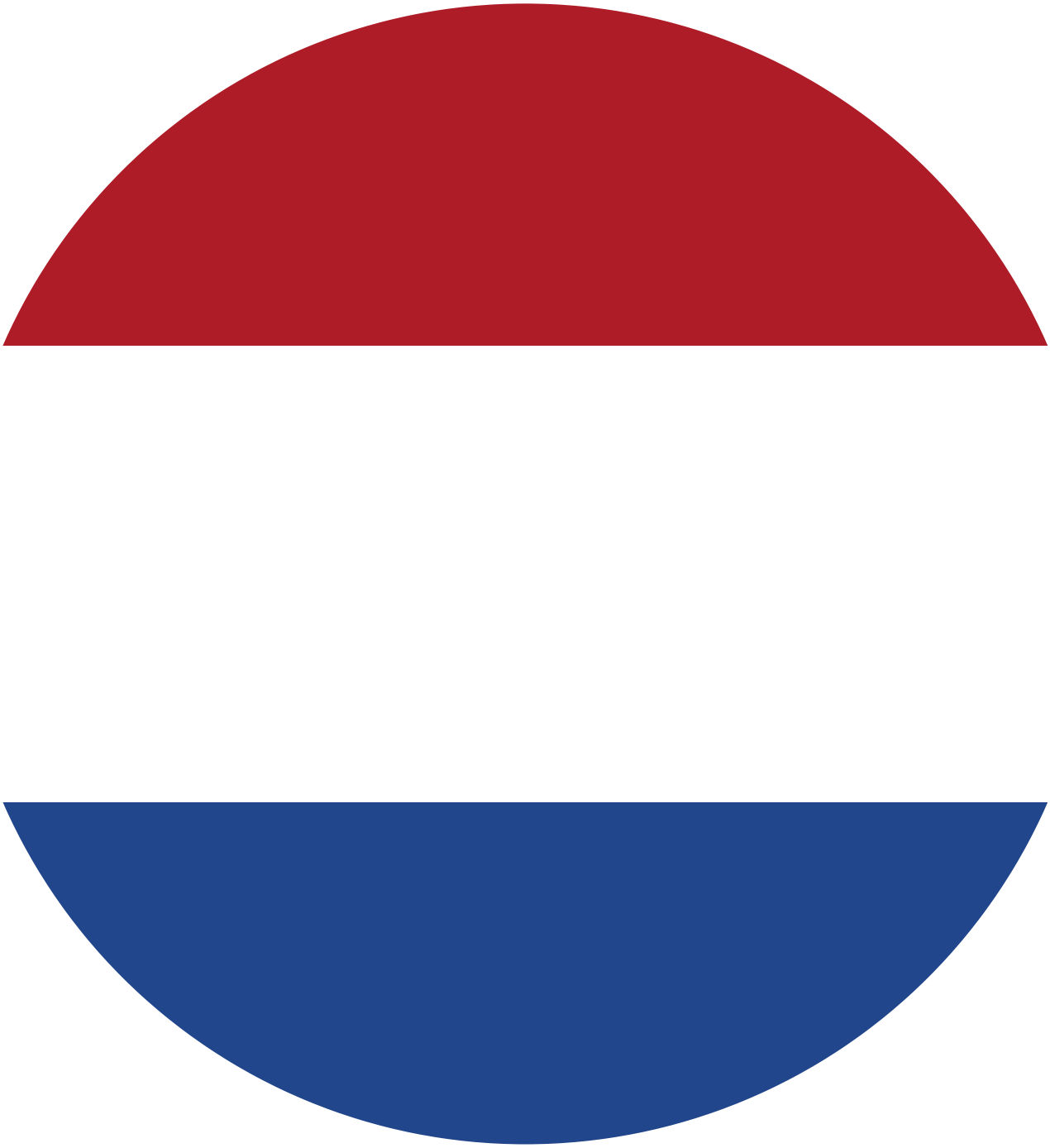
- België

- Suisse

- Schweiz



- Nederland



- Netherlands
- Deutschland
- Germany

- Österreich

CITY OF OAKLAND

Memorandum

TO: Darren Allison
Interim Chief of Police

FROM: Drennon Lindsey, Deputy Chief
OPD, Bureau of Investigations

SUBJECT: Automated License Plate Reader – 2022 Annual Report

DATE: June 27th, 2023

Background

Oakland Police Department (OPD) ALPR Policy 430 (430.8 Agency Monitoring and Controls) states that the "ALPR Coordinator shall provide the Chief of Police and Public Safety Committee with an annual report for the previous 12-month period." Policy 430 precedes City Council adoption of the Surveillance Technology Ordinance, enshrined in Oakland Municipal Code (OMC) 9.64; OMC 9.64 separately also requires annual reports as well as review and recommendation of a Surveillance Use Policy (SUP) and Surveillance Impact Report (SIR) – referred to collectively as "Privacy Policy."

OPD received approved ALPR policy DGO I-12 in October 2022. After that meeting, OPD started the process to upgrade the servers to improve auditing functionality. Unfortunately, legal advised that OPD still needed to go through a normal contract process to purchase the upgrade. This purchase approval was not obtained until late November 2022. At the same time, OPD was told by the vendor that we would now need new servers to host the upgraded software. OPD investigated purchasing new hardware, which was not feasible due to a server hardware shortage. At this point, OPD inquired about hosting the upgrade through a virtual machine, which took us into December 2022.

In parallel, OPD began to evaluate the feasibility of adhering to the policy with all the new requirements, which were not originally considered when discussion of the server upgrade began. Our legal team advised OPD that we not complete the upgrade until we were sure we could follow all the requirements in DGO I-12. OPD had several concerns around capturing all the data that was required in the new policy, which took us into 2023. OPD did not want to knowingly violate the new policy and the server upgrade was put on hold.

In early 2023, we had a leadership change, which was followed by a ransomware event which took ALPR offline in early February. OPD resources were also stretched thin during this time as the focus was on system restoration. Once the ALPR system was restored, OPD willingly left the system offline until we could meet with the PAC about our concerns in DGO I-12. After reviewing the policy, OPD has some minor suggestions and points of clarification we would like to discuss with the PAC.

2022 Annual Report Details

A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

Table 1 below shows the total scans and hits by month – the total license plate photographs made and stored each month (784,620 scans total for the year). Table 1 also shows the

number of times the vehicle-based systems had a match ("hit") with a California Department of Justice (CA DOJ) database (981 total for 2022). OPD's very outdated ALPR system can only quantify these two figures; the system can no longer quantify individual queries or perform any audit functions, as the software is no longer supported from the original vendor.

Table 1: 2022 OPD ALPR Scans and Hits

Month	Year	Scans	Hits
Jan	2022	119821	182
Feb	2022	86580	87
Mar	2022	116088	104
Apr	2022	99012	107
May	2022	96956	117
Jun	2022	47603	43
Jul	2022	38069	49
Aug	2022	18712	26
Sep	2022	54181	81
Oct	2022	62232	88
Nov	2022	26579	59
Dec	2022	18787	38
2022 Totals		**784,620**	**981**

B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

We had three requests for information and all three were approved. Details can be found in the attached spreadsheet titled ALPR External Requests Approval_2022.

C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to:

The ALPR cameras are installed upon fully marked OPD patrol vehicles (20 are operational but are currently not in use). Since the cameras are attached to specific vehicles, when a vehicle is involved in a collision or taken out of service due to age, we lose the use of the camera. The cameras are so old, that we cannot replace them with the same technology.

D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year:

When the system is active, these vehicles are assigned to the Bureau of Field Operations I (administered out of the Police Administration Building in downtown Oakland) as well as Bureau of Field Operations II (administered from the Eastmont Substation). The vehicles are deployed throughout the City in a patrol function to allow for large areas of the City to have ALPR coverage as the patrol vehicles are used to respond to calls for police service. Currently there are 15 systems in BFO 1 and 5 systems in BFO 2.

E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review:

Members of the public have spoken at PAC meetings regarding concerns of negative impacts to privacy protections (e.g., that OPD could use ALPR server data to establish travel patterns of particular vehicles associated with particular license plates, and/or that ALPR data can be inadvertently released through inadequate privacy protocols). OPD has also heard comments that more advanced ALPR systems may be used to track other vehicle attributes (e.g., bumper stickers). More recently, OPD staff have also heard from members of the public in support of ALPR systems and wanting to be sure that OPD utilizes technology appropriately to support OPD investigations. Furthermore, OPD personnel are aware of media reports of ALPR systems where a lack of updates between local systems and State CA DOJ databases lead to inaccurate stolen vehicle notifications, which have led law enforcement to stopping motorists because of stolen vehicle notifications.

OPD is not able to provide the race of each person connected to each ALPR scan. Race data is not captured in the scan itself as explained in the ALPR Draft Surveillance Impact Report. Race data would only be captured if there is a related criminal investigation for a particular ALPR scan capture. Staff could attempt to connect each scan to the associated vehicle registration of each scanned license plate. However, staff would not know if the vehicle driver, at the time of the ALPR scan, is the same person as the registered owner of the vehicle. Furthermore, staff believes that the potential for greater invasiveness in capturing this data outweighs the public benefit of capturing the data. Staff therefore recommend that the PAC makes the determination, that the administrative burden in collecting or verifying this information as well as the associated potential for greater invasiveness in capturing such data outweighs the public benefit.

F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information:

The current system is outdated, and the software is not supported from the original vendor. Prior to this loss in function, the system could be used to run reports for sample audits that detailed the reasons for queries (e.g., type of criminal investigation). When active, the ALPR system can currently quantify only hit and scan data. The upgrade to improve audit functionality was put on-hold to ensure OPD could adhere to the new policy.

G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response:

There were no identifiable data breaches or unauthorized access during the year of 2022.

H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes:

The ALPR system has two purposes. The first purpose is the real time alert for vehicles on a hotlist. Appendix A below, shows cases in which the ALPR system has been instrumental in recovering stolen and carjacked vehicles. The second purpose is the ability to locate where an individual might be based on past vehicle location data. At this time, it is difficult to ascertain the effectiveness for this query function due to the process of collecting data being manual and very labor intensive. OPD was unable to find any definitive cases where our ALPR helped on an active investigation for 2022.

I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates:

OPD had three public records requests regarding ALPR technology and data:

- *The first request (22-7205 Request for specific plate and location data) was denied per Gov. Code § 6254 (c).*
- *The second request (22-8523 Electronic Frontier Foundation) was completed and closed.*
- *The third request is 22-2640 (Espler Foundation) and was completed and closed.*

J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year:

Zero; OPD did not incur any maintenance, licensing, or training costs. Training is completed using OPD's online portal as well as staff time.

K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request:

OPD would like to potentially revisit our data sharing policy to explicitly include entities such as the district attorney or others who require ALPR data as evidence in a criminal case.

OPD is committed to providing the best services to our community while being transparent and instilling procedural justice through daily police activity. This report is compliance with these OPD commitments. OPD hopes that this report helps to strengthen our trust within the Oakland community.

Respectfully submitted,

_____

Darren Allison,
Interim Chief of Police

Reviewed by,
David Elzey, Acting Deputy Chief
OPD, Bureau of Investigations

Dr. Carlo Beckman, Police Services Manager
OPD, Research and Planning Section

Prepared by:

David Pullen, Officer
OPD, Bureau of Services, IT Unit

Tracey Jones, Manager
OPD, Bureau of Services, Research and Planning

Appendix A

Sample of stolen vehicles recovered using ALPR technology

For all the examples below, officers performed necessary verification of the stolen vehicle status before acting.

1. 22-054545 11/27/22 ALPR hit on parked stolen vehicle out of Berkeley. Vehicle Recovered. LOCATION OF RECOVERY: 550 42nd St, DATE OF THEFT: 11/15/22, VEHICLE DESCRIPTION: 2013 Nissan Leaf 4D Mar
2. 22-053508 11/26/22 ALPR hit on parked stolen vehicle out of Oakland. Vehicle Recovered. LOCATION OF RECOVERY: 5700 Miles Ave, DATE OF THEFT: 11/19/22, VEHICLE DESCRIPTION: 1990 Honda Accord 4D Whi
3. 22-054335 11/25/22 ALPR hit on parked stolen vehicle out of Oakland. Vehicle Recovered. LOCATION OF RECOVERY: 5532 Vincent Way, DATE OF THEFT: 11/25/22 VEHICLE DESCRIPTION: 2014 Kia Sorento SUV Whi
4. 22-051892 11/12/22 ALPR hit on parked stolen vehicle out of Oakland. Vehicle Recovered. LOCATION OF RECOVERY: 3400 Elm St, DATE OF THEFT: 11/11/22 VEHICLE DESCRIPTION: 2021 Honda Accord 4D Whi
5. 22-048549 11/05/22 ALPR hit on parked stolen vehicle out of Oakland. Vehicle Recovered. LOCATION OF RECOVERY: 4600 Dover St, DATE OF THEFT: 10/21/22 VEHICLE DESCRIPTION: 2017 Hyundai Elantra 4D Sil
6. 22-050649 11/04/22 ALPR hit on parked stolen vehicle out of San Francisco. Vehicle Recovered. LOCATION OF RECOVERY: 550 30th St, DATE OF THEFT: 10/21/22 VEHICLE DESCRIPTION: 2016 Hyundai Elantra 4D Blk
7. 22-047320 10/28/22 ALPR hit on parked stolen vehicle out of Oakland. Vehicle Recovered. LOCATION OF RECOVERY: 3400 Richmond Blvd DATE OF THEFT: 10/14/22 VEHICLE DESCRIPTION: 2000 Chevrolet S10 Pickup Blk
8. 22-046146 10/20/22 ALPR hit on parked stolen vehicle out of Oakland. Vehicle Recovered. LOCATION OF RECOVERY: 3300 Blk E 9th St, DATE OF THEFT: 10/08/22 VEHICLE DESCRIPTION: 2000 Toyota Corolla 4D Grn
9. 22-047096 10/14/22 ALPR hit on parked stolen vehicle out of Berkeley. Vehicle Recovered. LOCATION OF RECOVERY: 2300 Telegraph Ave, DATE OF THEFT: 10/12/22 VEHICLE DESCRIPTION: 1993 Honda Accord 4D Whi
10. 22-046445 10/10/22 ALPR hit on parked carjacked vehicle out of Fremont. Vehicle Recovered. LOCATION OF RECOVERY: 550 Blk 30th St, DATE OF THEFT: 09/23/22 VEHICLE DESCRIPTION: 2008 Toyota Prius 4D Gry
11. 22-042676 10/10/22 ALPR hit on parked stolen vehicle out of Oakland. Vehicle Recovered. LOCATION OF RECOVERY: 3800 Blk Maila Ave, DATE OF THEFT: 09/17/22 VEHICLE DESCRIPTION: 2016 Kia Soul 4D Blu
12. 22-044997 10/02/22 ALPR hit on occupied moving vehicle stolen out of Union City. Vehicle was stopped and the driver was arrested. Vehicle Recovered. LOCATION OF RECOVERY: 3600 Blk MLK Jr Way, DATE OF THEFT: 08/23/22 VEHICLE DESCRIPTION: 1997 Honda Accord 2D Gry
13. 22-044986 10/01/22 ALPR hit on parked stolen vehicle out of El Cerrito. Vehicle Recovered. LOCATION OF RECOVERY: 3700 Shafter Ave, DATE OF THEFT: 08/18/22 VEHICLE DESCRIPTION: 1995 Honda Del Sol 2D Whi

14. 22-043082 10/01/22 ALPR hit on parked stolen vehicle out of Oakland. Vehicle Recovered. LOCATION OF RECOVERY: 3612 Webster St, DATE OF THEFT: 09/20/22 VEHICLE DESCRIPTION: 2002 Saturn LS 4D Gold
15. 22-044025 09/26/22 ALPR hit on parked stolen vehicle out of Berkeley. Vehicle Recovered. LOCATION OF RECOVERY: 5100 Broadway, DATE OF THEFT: 09/06/22 VEHICLE DESCRIPTION: 1997 Subaru Impreza SW Red
16. 22-032484 07/18/22 ALPR hit on parked stolen vehicle out of Oakland. Vehicle Recovered. LOCATION OF RECOVERY: 1400 13th St, DATE OF THEFT: 07/16/22 VEHICLE DESCRIPTION: 2018 Kia Sol 4D Gry
17. 22-016439 05/02/22 ALPR hit on parked carjacked vehicle out of Oakland. Vehicle Recovered. LOCATION OF RECOVERY: 2100 Blk Santa Rita St, VEHICLE DESCRIPTION: 2003 BMW 745Li Blu
18. 22-018861 04/24/22 ALPR hit on parked stolen vehicle out of Berkeley. Vehicle Recovered. LOCATION OF RECOVERY: 3500 Blk Webster St, DATE OF THEFT: 04/23/22 VEHICLE DESCRIPTION: 1997 Ford F150 PK Gry
19. 22-016985 04/12/22 ALPR hit on occupied moving vehicle with a felony want attached to the plate for felony evading out of Hayward. Vehicle fled from officers and was stopped by SFPD. OPD officers responded and arrested occupants for drugs and weapons violations. Vehicle Recovered. LOCATION OF RECOVERY: 23rd Ave & E 17th St, VEHICLE DESCRIPTION: 2010 Mercedes 300 4D Sil
20. 22-013139 04/10/22 ALPR hit on parked stolen vehicle out of Oakland. Vehicle Recovered. LOCATION OF RECOVERY: 300 27th St, DATE OF THEFT: 03/20/22 VEHICLE DESCRIPTION: 2001 GMC Sierra PK Whi
21. 22-015601 04/04/22 ALPR hit on parked stolen vehicle out of Berkeley. Vehicle Recovered. LOCATION OF RECOVERY: 560 33rd St, DATE OF THEFT: 03/11/22 VEHICLE DESCRIPTION: 1998 Mercury Tracer 4D Whi
22. 22-015157 04/01/22 ALPR hit on occupied moving vehicle stolen out of Hayward. The vehicle was stopped and the driver was arrested. Vehicle Recovered. LOCATION OF RECOVERY: 1300 Blk International Blvd, DATE OF THEFT: 03/24/22 VEHICLE DESCRIPTION: 2002 Chevrolet SLV PK Blk
23. 22-012811 03/18/22 ALPR hit on parked stolen vehicle out of Richmond. Vehicle Recovered. LOCATION OF RECOVERY: 5400 Lowell Ave, DATE OF THEFT: 02/14/22 VEHICLE DESCRIPTION: 2005 Chevrolet Tahoe SUV Gld
24. 22-009323 02/26/22 ALPR hit on parked stolen vehicle out of San Francisco. Vehicle Recovered. LOCATION OF RECOVERY: 5700 Presley Way, DATE OF THEFT: 02/07/22 VEHICLE DESCRIPTION: 2002 Chevrolet Tahoe SUV Grn
25. 22-003836 02/02/22 ALPR hit on parked stolen vehicle out of Oakland. Vehicle Recovered. LOCATION OF RECOVERY: 5100 Blk E 10th St, DATE OF THEFT: 01/24/22 VEHICLE DESCRIPTION: 2003 Chevrolet Silverado 2500 Whi
26. 22-052415 11/20/22 ALPR hit on parked stolen vehicle out of Oakland. Vehicle Recovered. LOCATION OF RECOVERY: 3300 Blk Piedmont Ave, DATE OF THEFT: 11/13/22 VEHICLE DESCRIPTION: 2002 Honda Accord Blk
27. 22-045837 11/04/22 ALPR hit on parked stolen vehicle out of Oakland. Vehicle Recovered. LOCATION OF RECOVERY: 1310 Mountain Blvd, DATE OF THEFT: 10/06/22 VEHICLE DESCRIPTION: 2009 Toyota Camry 4D Whi
28. 22-021730 11/01/22 ALPR hit on parked carjacked vehicle out of Oakland. Vehicle Recovered. LOCATION OF RECOVERY: 2300 Blk 17th Ave, DATE OF THEFT: 05/10/22 VEHICLE DESCRIPTION: 2021 Honda HRV SUV Whi

29. 22-046932 10/15/22 ALPR hit on parked stolen vehicle out of Oakland. Vehicle Recovered. LOCATION OF RECOVERY: 200 Blk 28th St, DATE OF THEFT: 10/13/22 VEHICLE DESCRIPTION: 2016 Hyundai Elantra 4D Red
30. 22-046080 10/07/22 ALPR hit on parked stolen vehicle out of Alameda County. Vehicle Recovered. LOCATION OF RECOVERY: 2600 Blk Northgate, VEHICLE DESCRIPTION: 1999 Chevrolet Silverado PK Mar
31. 22-039824 09/09/22 ALPR hit on parked stolen vehicle out of Oakland. Vehicle Recovered. LOCATION OF RECOVERY: 800 Blk 5th St, DATE OF THEFT: 08/31/22 VEHICLE DESCRIPTION: 2001 Subaru Forrester 4D Gld
32. 22-029782 06/30/22 ALPR hit on parked stolen vehicle out of CHP Solano. Vehicle Recovered. LOCATION OF RECOVERY: 500 Blk Broadway, VEHICLE DESCRIPTION: 2002 Chevrolet C2500 PK Gry
33. 22-018323 05/12/22 ALPR hit on parked carjacked vehicle out of Oakland. Vehicle Recovered. LOCATION OF RECOVERY: 2400 Blk 12th Ave, DATE OF THEFT: 04/20/22 VEHICLE DESCRIPTION: 2015 BMW 428i 4D Blk
34. 22-013617 03/24/22 ALPR hit on parked stolen vehicle out of Oakland. Vehicle Recovered. LOCATION OF RECOVERY: 1904 Franklin St, DATE OF THEFT: 03/22/22 VEHICLE DESCRIPTION: 2004 Toyota Corrola 4D Blk

Changes in order of appearance (and importance).

1.

A. Authorized Uses: *The specific uses that are authorized, and the rules and processes required ~~prior to such use~~.*

Deletion of "prior to such use" as it is inconsistent between historical and real-time use.

2.

(1) Department members will ~~clear~~ document all stops from hot list alerts by indicating the positive ALPR Hit, i.e., with an arrest or other enforcement action on a computer generated spreadsheet that shall include at minimum a) the Department member's name that responded to the alert, b) the justification for responding to the alert, c) the related case number, d) the disposition code, e) time and date of the response, and f) and any known next steps or follow up (e.g. forwarding case to District Attorney, alerting owner to recovered stolen vehicle).

Substitution of "document" for "clear" to remove confusion on time standards.

See comment in DGO.

3.

1. Data will be transferred from ~~vehicle~~ LPRs to the designated storage per the automated ALPR technology data transfer protocol.

Substitution of "LPRs" for "vehicle" for precision and deletion of automated for redundancy.

4.

ALPR system audits shall be conducted annually to ensure proper system functionality and that personnel are using the system according to policy rules via sample audits, and reviews of training records.

Addition of "and" and a period to correct error.

Considerations

1. As to section K. Auditing and Oversight:
    a. We are assuming that the quarterly report is based on samples – see the comment in the DGO.
    b. As this section only requires a sample for audit, OPD can gather these results given a reasonable sample size. Recommend audit of 10-15 incidents. A

random audit will include incidents that are not completed, thus not necessarily productive for an analysis of efficacy. OPD can take a sample of completed incidents for additional efficacy review in the quarterly reports.

2. As to Section B Authorized Uses, (2)
    a. OPD can create this spreadsheet by requiring all stops based in part by ALPR to include "alpr_stop" to be written in the admin section. This will be searchable and able to be linked with LRMS systems to satisfy all of the requirements in this section.

DEPARTMENTAL GENERAL ORDER

I-29: Fixed-Wing Aircraft Mounted Camera Surveillance Use Policy

Effective Date: DD MMM YY
Coordinator: Special Operations Division

COMMAND INTENT

The Oakland Police Department believes in protecting and serving its diverse community and city through fair, equitable, and constitutional policing. OPD believes in the usage of technology to aid in this mission and in the investment into progressive forms of surveillance technology which both protects the unassailable rights of members of the community, while also ensuring and enhancing the safety of community members, officers, and engaged persons. This includes a multipronged approach related to tactics, methodology, and technology that allows for de-escalation in often rapidly evolving and tumultuous environments.

At the direction of the Oakland City Council, Oakland Public Safety Committee, Reimagining Public Safety Task Force, and the Oakland Police Department, the Air Support Unit has explored numerous alternatives to the current methods and equipment utilized by the Air Unit. After careful consideration, product testing/evaluation, fiscal analysis, stakeholder input, and industry standards, the Department requested that a fixed-wing aircraft be purchased for use by the Air Support Unit. The use of a fixed-wing aircraft necessitates the utilization of an Aircraft Mounted Camera (AMC) which allows a Flight Observer (FO) to observe, document, and relay the events occurring on the ground, to responding officers, partnering first responders, supervisory and command members, and other relevant stakeholders, with the purpose of providing enhanced public safety while also ensuring overall accountability related to department members and engaged persons.

A. Description and Purpose of the Technology

A - 1. Aircraft Mounted Camera Systems (AMC)

The fixed-wing aircraft operates at a significantly higher altitude than the rotary-wing aircraft (helicopter) utilized by the department (fixed-wing aircraft operates at 3000+ ft above ground level (AGL); helicopter operates at 500-700 ft. AGL). The fixed-wing aircraft aims to reduce noise/light pollution as well as work to limit potential trauma incurred by the community members of Oakland who may have a negative association with or reaction to the sound of the department rotary wing aircraft (helicopter).

A byproduct of the higher altitude of the fixed-wing aircraft is that a FO can no longer rely on observing, with the unaided eye, through the window of the aircraft to make accurate and beneficial observations as to what is occurring

on the ground. The FO must instead rely on a high-definition pan-tilt-zoom camera, specially designed for use at altitude, and mounted onto the body of the aircraft.

An aircraft mounted camera system (AMC) will need to be utilized throughout the entirety of the flight while responding to assist with dispatched calls, critical incidents, search and rescue operations, mitigating vehicle pursuits (allowing ground units to disengage), and a variety of other roles previously conducted by the department's rotary wing aircraft. Aircraft mounted cameras (AMCs) have been utilized on the department's rotary-wing aircraft (helicopter) for over two decades. The current AMC technology, however, is outdated and is largely ineffective to perform the evolving objectives of the Air Support Unit.

A - 2. Downlink System Component

The Downlink component of the system allows the video and pictures captured by the AMC to be streamed via a secure wireless connection to those devices authorized and approved by the department. Downlink is functional whether the AMC is operating in the passive or active recording modes. Utilizing Downlink offers the opportunity to provide department members, city leaders, and other emergency responders with a greater overall picture of what is occurring during critical incidents. This has the potential to provide valuable information allowing for more informed decisions that enhance the safety of the community and first responders. Downlink has the capability of being utilized during natural disasters (e.g., earthquakes, fires, flooding etc.) to allow emergency personnel to assess evacuation routes, direct responders, and coordinate emergency efforts.

The Downlink component can also be used to ensure more effective command and control and enhanced accountability during critical incidents and crowd control events[1]. Utilization during crowd control events would aim to reduce the need for officers to be in direct contact with large crowds in the event there are a small number of violent agitators who conceal themselves within a group of peaceful demonstrators, as has been observed during previous crowd control events. Downlink allows commanders a comprehensive overview with which to plan field operations that focus on safely facilitating members of the community being able to demonstrate and exercise their constitutional rights in public spaces. The live feed will allow commanders to coordinate appropriate traffic control to safely facilitate marches, respond to medical emergencies within the crowd, and when necessary, safely plan the

[1] Any recordings captured during crowd control events shall be taken and managed in accordance with Training Bulletin III – G.

apprehension of specific agitators who pose a danger to the community or significant property, while at the same time, limiting the potential impact on the overall group.

Downlink will also play a critical role in responding to unlawful, dangerous, and often violent sideshow activity throughout the City of Oakland. The use of Downlink in these circumstances will facilitate the documentation of dangerous unlawful activities conducted by participants in sideshow events, as well as provide critical information to commanders which will be used in planning the Department's measured response.

A - 3. Aircraft Mounted Camera Modes

The Aircraft Mounted Camera (AMC) has several modes in which it can be operated. These modes can be separated into two major categories:

- Color Camera: Used during daytime operations and provides High-Definition Color video and still images to the Flight Observer (FO) monitoring the images within the aircraft.
- Infrared (IR) Camera: Used to search for heat signatures during low light/visibility conditions. Infrared is an energy similar to visible light, but with a longer wavelength. Infrared energy is invisible to the human eye, however, while visible light energy is emitted by objects only at a very high temperature, infrared energy is emitted by all objects at ordinary temperatures. Since thermal imagers sense infrared energy, which varies with the temperature of objects in a scene, the image generated provides a thermal signature of the scene. This image can be displayed on a standard video monitor.

Infrared energy from objects on a scene are focused by optics onto an infrared detector. The infrared information is then passed to sensor electronics for image processing. The signal processing circuitry translates the infrared detector data into an image that can be viewed on a standard video monitor.

Thermal imaging systems not only make it possible for FO's to make observations in the dark but also enhance the ability of the FO to detect critical objects not visible otherwise. Warmer objects such as people and animals stand out from typically cooler backgrounds. This allows a FO to provide critical information to ground units, which may prevent surprise chance encounters between officers and an engaged person or an aggressive animal, both of which may be avoided by creating time and distance by way of the Air Unit's observations. Thermal imaging systems are significantly

more effective than the unaided eye in daylight, night, and most poor weather conditions. IR cameras *cannot* see through walls, rooftops, or glass. However, IR cameras are capable of seeing through smoke which can be critical in a firefighting or rescue environment.

Either of these modes can be recorded and stored digitally on a hard drive for later upload and can also be transmitted via Downlink as approved within this policy.

B. Use of the Aircraft Mounted Camera (AMC)

B - 1. AMC Recording Modes (Active/Passive)

Active recording is defined as initiating the visual recording capabilities of the AMC. When the AMC is not actively recording, it is passively recording video in a 30-second continuous moving loop, often referred to as a 30-second rollback. When the AMC recording is activated by the operator, it saves this video-only (no audio) clip of the 30-second period prior to activation. This technology is functionally similar to the Department's Body Worn Camera (BWC) policy DGO I-15.

The AMC will be utilized during the entirety of the flight to enable the FO to monitor activity on the ground. Unlike the rotary wing helicopter, the FO in an airplane does not have the ability to look out the window and effectively observe actions on the ground due to the low wing design of the airplane as well as the altitude that the aircraft will typically be operating at: 2500-4500 feet above ground level (AGL). FO's frequently observe crimes and other incidents such as reckless driving, vehicles fleeing the scene of a violent felony, vehicle collisions, fires, etc., in public areas throughout the city. In many instances, the Air Unit is capable of responding to an incident prior to the arrival of ground units. This allows the Air Unit to provide critical information to units on the ground such as the location and condition of a victim of a shooting, a person injured from a significant collision, or even incidents of a missing person. In other incidents, the Air Unit may be able to advise of the location of a potential suspect related to a violent crime and information which may allow officers to respond with special consideration for creating time and distance from a potentially armed subject, key elements of de-escalation and preventing violent confrontations between an armed engaged person and officers. Without the ability to effectively observe these incidents, officers cannot relay critical information to dispatch, thereby delaying emergency response.

Once the AMC is placed in the active recording mode, the observations made by the AMC will be recorded continuously until the FO deactivates the recording or the data storage device is full. It should be noted that, unlike the BWC, the AMC does not capture live audio in conjunction with the video recording. The AMC is capable of capturing radio traffic which is synced with the video at the time of the recording.

Each time the camera is turned off or placed in a storage condition the device will experience a delay, up to several minutes, in order to realign itself with the aircraft and recalibrate the onboard sensors. These delays could cause significant information/data to be uncaptured during a critical incident which could adversely influence the outcome of the investigation and those involved. For this reason, while operating the aircraft the AMC shall be maintained in the passive mode or active recording mode while the aircraft is in flight and operating in a potential enforcement capacity.

B - 2. Required Activation of the AMC

Members operating the AMC shall activate the recording function on the AMC camera while making observations in the following circumstances:

1. Members are actively involved in a detention and/or arrest and this information is known to the operator of the AMC;
2. Members are actively conducting a search of a yard, building, area, or vehicle, where a suspect is anticipated to be located or to rule out the presence of a suspect.[2]
3. While members are conducting an assessment or evaluation for a psychiatric detention pursuant to Welfare and Institutions Code § 5150, and where the engaged subject has been observed as actively violent towards community members or officers;
4. Members on the ground are engaged in a pursuit, as defined in DGO J-04, *Pursuit Driving;*
5. The Air Unit is actively engaged in following a vehicle following the termination of a pursuit or other criminal activity, where enforcement action by ground units is pre-planned or imminent;
6. While members are actively serving a search or arrest warrant and the

[2] This does not include situations where officers are conducting a perimeter for a prolonged period, where a search is not actively being conducted, and the actions of the suspect are not able to be observed by the Flight Operator.

location has not yet been determined to be secured;

7. When members are observed taking any enforcement action or when the AMC operator is directed to activate the recording feature by a supervisor or commander during a crowd control situation in the City of Oakland (*Training Bulletin III-G*).

B - 3. Deactivation of the AMC

Once activated pursuit to B-2, Members shall not deactivate the AMC recording until one of the following occurs:

1. It is determined by ground units or the AMC operator that there is no person related to criminal activity present at the scene of the incident and anticipation of contact with such persons is unlikely;
2. The Air Unit's involvement in the contact, detention, search, or arrest has concluded;
3. Members have concluded a search of a yard, building, area, or vehicle, and are no longer actively searching for a suspect, or in situations where the Air Unit is no longer involved in a search;
4. The Air Unit terminates its involvement in following a vehicle that was involved in a pursuit or other criminal activity;
5. They receive an order from a higher-ranking member. That higher ranking member shall note the reasoning for deactivation via Computer Aided Dispatch (CAD), their BWC, or report;

If circumstances arise requiring re-activation members shall re-activate pursuant to B-2, above.

B - 4. Prohibited Use

1. AMC shall not be equipped with analytics capable of identifying groups or individuals, including but not limited to Artificial Intelligence, facial recognition, gait analysis, or Automated License Plate Reader (ALPR).
2. AMC shall not be used for the following activities:
   a. Conducting surveillance of anyone not subject to an active investigation.
   b. Targeting a person or group of people based on their characteristics, such as but not limited to race, ethnicity, national origin, religion, disability, gender, clothing, tattoos, sexual orientation and/or perceived affiliation when not connected to actual information about specific individuals related to criminal investigations.
   c. For the purpose of harassing, intimidating, or discriminating against any individual or group.

d. To conduct personal business of any type.

B - 5. Discretionary Activation

When not required to activate or prohibited from activation as described above (see B - 2- and B - 3), members may use their discretion when deciding to activate or de-activate the AMC recording functionality if it is in furtherance of an active investigation and serves a legitimate law enforcement purpose.

B - 6. Privacy Considerations

AMC Operators shall not intentionally record or transmit images of any location where a person would have a reasonable expectation of privacy (e.g., residence, yard, enclosure) without a search warrant unless exigent circumstances exist.

When OPD Aircraft are being flown and the AMC is being utilized, operators should take steps to ensure the camera is focused on the areas that are necessary to the task and to minimize the inadvertent collection of data about uninvolved persons or places. Operators and observers shall take reasonable precautions, such as being conscious and deliberate with the positioning of an imaging device, to avoid inadvertently recording or transmitting images of areas where there is a reasonable expectation of privacy.

B - 7. AMC Use Documentation

Members are required to document all activations of the AMC, except for tests or accidental recordings. Documentation shall be made in the Aircraft Flight Log (TF-488A). Delayed or non-activations of the AMC, when activation was required by policy, shall be documented in the appropriate report, and reported to the member's supervisor.

B - 8. Data Upload

Members shall upload AMC data files (videos) at the conclusion of their shift, or if directed by a supervisor, during their shift, to ensure local storage capacity is not exceeded.

B - 9. Annotation and Categorization of AMC Files

All members shall annotate AMC data files (videos) daily, or, if not feasible, by the end of the member's next regularly scheduled workday. The following information shall be annotated on every AMC data file:

- The report number associated with the incident recorded (in the ID field);
- or the incident number (in the ID field if there is no report number associated with the incident being recorded).
- The category of the video using the appropriate retention category (on Evidence.com).

If neither the report number nor the incident number exists, members may use the letters "NA" or leave the ID field blank. Members are authorized to view their video in order to identify the file for annotation unless otherwise prohibited by policy. During incidents that require exceptional resources or large-scale activation of Department members (e.g. natural disaster), the incident commander may approve delayed annotation of AMC files except in cases that require an investigative call-out. The incident commander shall document any such orders in the appropriate after-action report.

C. AMC Data Management

C - 1. Data Collection

The activation and deactivation of the recording capabilities and subsequent data collection shall be in accordance with sections B - 2 through B - 5 of this policy. The AMC operator will maintain the integrity of a dedicated AMC data storage device and shall not overwrite or delete the video files contained within, until which time the data is uploaded onto the Evidence.com servers.

C - 2. Court and Judicial Proceeding AMC File Copies

Personnel requiring a copy of AMC audio/video file(s) for court (e.g., for Traffic court, or a proceeding in a different county) shall contact their first line supervisor or their designated System Administrator (for non-patrol assignments). If the first line supervisor is unavailable, personnel shall contact any System Administrator. Any AMC copies not entered into evidence shall be returned to the first line supervisor or a System Administrator for destruction.

CID and other investigative personnel taking a case to the District Attorney (DA) for charging are responsible for obtaining copies of, and/or using the evidence.com secure sharing capability to share, all applicable AMC files for presentation to the DA.

Prior to copying the AMC video file, members authorized to make copies shall document the reason for making the copy and the name of the person receiving the copy in the "Notes" field of each video file copied. If applicable, the name entry shall also include the person's rank and serial number. The person receiving the copy shall maintain the copy in a secure location until it is needed for court or custody is transferred to another person. Additionally, they shall document, as soon as practical, the name and/or position of the person receiving the copy in the "Notes" field of each video file.

The documentation of the chain of custody and responsibility to secure the copy shall transfer to the person receiving the copy until:

- The copy is received by non-Department personnel (e.g. District Attorney, City Attorney, Court Clerk, etc.);
- The copy is admitted into evidence; or
- The copy is returned to a system administrator for destruction.

C - 3. Use of AWC Files for Training

Training staff is authorized to view AMC files regarding incidents which may serve as learning or teaching tool. An AMC file may be utilized as a training tool for individuals, specific units, or the Department as a whole. A recommendation to utilize a AMC file for such a purpose may come from any source.

A person recommending utilizing a AMC file for training purposes shall submit the recommendation through the chain of command to the Training Section Commander.

The Training Section Commander shall review the recommendation and determine how best to utilize the AMC file considering the identity of the person(s) involved, sensitivity of the incident, and the benefit of utilizing the file versus other means.

C - 4. Additional Data Access

Outside of the provisions described in C – 2, AMC image and video data that is recorded and stored within the removable drive or on AXON may be shared only with other law enforcement or prosecutorial agencies for official law

enforcement purposes or as otherwise permitted by law, using the following procedures:

1. The agency makes a written request for the OPD data that includes:
   a. The name of the requesting agency.
   b. The name of the individual making the request.
   c. The basis of their need for and right to the information.
      i. A right to know is the legal authority to receive information pursuant to a court order, statutory law, or case law. A need to know is a compelling reason to request information such as direct involvement in an investigation.
2. The request is reviewed by the Chief of Police, Assistant Chief of Police, Deputy Chief/ Deputy Director, Criminal Investigations Division Commander or designee and approved before the request is fulfilled.
3. The approved request is retained on file, and incorporated into the annual report pursuant to Oakland Municipal Code Section 9.64.010 1.B.

C - 5. Data Protection and security

All AMC data storage devices (SD Card, Flash Drive, Portable Hard Drive) will be secured in a manner (e.g. lockbox) only accessible to Air Support Unit (ASU) personnel. All evidence from ASU data devices shall be uploaded to the Evidence.com server and then immediately removed from the drive.

C - 6. Data Retention

In line with the existing DGO I-15- Body Worn Camera (BWC) Policy, which utilizes the same cloud storage platform (Evidence.com) AMC files shall be retained for a period of two years unless it is required for:

1. A criminal investigation;
2. An administrative investigation;
3. Research;
4. Civil litigation;
5. Training; and/or
6. No recordings shall be deleted while any request for the recordings is pending, including but not limited to a public records request or litigation hold request

AMC files that are not flagged for retention for any of the above reasons

will be automatically deleted by the File Management System's data retention processes, which are set and maintained by the Project Administrator or designee. This retention process is already in place and utilized for BWC data.

C - 7. Public Access

AMC data which is collected and retained under section C - 6 of this document is considered a "law enforcement investigatory file" pursuant to Government Code § 6254, and shall be exempt from public disclosure. The Department will disclose recordings as appropriate pursuant to statute or court order. AMC data which is retained pursuant to section C - 6 shall be available via public records request pursuant to applicable law regarding Public Records Requests as soon as the criminal or administrative investigations has concluded and/or adjudicated.

D. ADMINISTRATIVE INFORMATION

D - 1. Training

The ASU Unit Supervisor, or other designated OPD personnel, shall ensure that all authorized operators and required observers have completed all department-approved training in the operation, applicable laws, policies and procedures regarding the use of the AMC and downlink. This annual training will be documented utilizing a policy compliance attestation form to be created upon implementation of this policy.

D - 2. Auditing and Oversight

The ASU unit supervisor, or other designated OPD personnel, shall develop a protocol for documenting all AMC uses in accordance to this policy with specific regard to safeguarding the privacy rights of the community and include this in the AMC procedure manual and the annual AMC report. The ASU supervisor will develop an electronic record of deployments and recordings created. The operator of the AMC will document the deployments in the appropriate flight logs. This protocol will allow the ASU supervisor to have a continuous log of all deployments and assist with completing the annual report.

D - 3. Maintenance

The ASU unit supervisor, or other designated OPD personnel, shall develop an AMC inspection, maintenance, and record keeping protocol to ensure the

continuing functionality of the AMC, and include this protocol in the AMC procedure manual. Maintenance and record-keeping should also include expenditures such as purchase of new equipment, required updates and mechanical repairs.

D - 4. Description of the Technology AMC File Management System

The AMC system employed by OPD features upload computer stations and an internet web interface for controlling how files are uploaded and archived. The interface allows for Internet Protocol restriction features to control the locations where the system can be accessed. These restrictions limit AMC video file access to only authorized OPD personnel. Videos that are tagged for any reason as part of an investigation are moved to separate folders where they cannot be deleted. The cloud-based archive system has built-in redundancy with multiple servers to ensure data integrity and CJIS compliance.

By order of

Darren Allison
Interim Chief of Police Date Signed: _____

DEPARTMENTAL GENERAL ORDER

I-12: AUTOMATED LICENSE PLATE READERS

Effective Date: 18 Oct 22
Coordinator: Information Technology Unit

This policy provides guidance for the capture, storage and use of digital data obtained through the use of ALPR technology while recognizing the established privacy rights of the public.

Definitions

(a) **Automated License Plate Reader (ALPR):** A device that uses cameras and computer technology to compare digital images of vehicle license plates to lists of known information of interest.

(b) **Hot List:** A list of license plates associated with vehicles of interest compiled from one or more databases including, but not limited to the Stolen Vehicle System (SVS), NCIC, and local BOLO alerts.

(c) **Hit:** Alert from the ALPR system that a scanned license plate may be in the National Crime Information Center (NCIC) or other law enforcement database for a specific reason including, but not limited to, being related to a stolen car, wanted person, missing person or domestic violence protective order.

A. Description of the Technology: *Information describing the surveillance technology and how it works.*

OPD uses Automated License Plate Reader (ALPR) technology to capture and store digital license plate data and images. There are two components to the ALPR system:

1. Automated License Plate Readers: Device components include cameras which can be attached to vehicles or fixed objects and a vehicle-based computer that processes the photographs and compares the data against California Department of Justice (CA DOJ) hot lists. Data are transmitted for comparison (the hot lists are downloaded to the vehicle at the start of the patrol shift and then compared from that list). Authorized personnel can also manually enter license plates to internal OPD generated hot lists only accessible to personnel authorized to access the OPD ALPR system.
2. ALPR Database: A central repository stores data collected and transmitted by the Automated License Plate Readers.

B. Purpose of the Technology

ALPR technology works by automatically and indiscriminately scanning all license plates on vehicles that are publicly visible. ALPR reads these license plates, compares

the license plate characters against Hot Lists, and stores the characters along with the date, time, and location where the photograph was taken. This process allows for two functions by ALPR:

1. Immediate (real time) comparison of the license plate characters against Hot Lists listing vehicles that are stolen or sought in connection with a crime and/or with OPD-generated internal lists.
2. Storage of the license plate characters – along with the date, time, and location where the photography was taken – in a database that is accessible to enforcement agencies with authorized access (as defined in "Authorized Use" below) for investigative query purposes.

C. Authorized Uses: *The specific uses that are authorized, and the rules and processes required.*

1. **Authorized Users**

Personnel authorized to use ALPR equipment or access information collected through the use of such equipment shall be specifically trained in such technology. Sworn personnel, Police Service Technicians, or other authorized Department personnel may use the technology. Authorized users other than sworn personnel or police services technicians (PST) must be designated by the Chief of Police or designee.

2. Authorized Use

(A) **Real-Time Identification**: The officer shall verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before possibly taking enforcement action that is based solely on an ALPR alert.

Once an alert is received, the operator shall confirm that the observed license plate from the system matches the license plate of the observed vehicle.

Members will not take any police action that restricts the freedom of any individual based solely on an ALPR alert unless it has been fully validated, by visually verifying that the license plate characters on the vehicle match those in the database, and that the make, model, color and all other known identifying characteristics likewise match.

(1) **Hot Lists**. The Department shall only use the following hot lists: Stolen Vehicle System ("SVS"), National Crime Information Center ("NCIC") lists, CA DOJ lists, Amber and Silver alerts, and custom BOLO lists pertaining solely to missing or at-risk persons, witness locates, and violent crime investigation. Hot lists shall be obtained or compiled from sources as may be consistent with the purposes of the ALPR system set forth in this Policy. Hot lists utilized by the Department's LPR system may be updated by agency sources more frequently than the Department may be uploading them and thus the Department's LPR system will not have access to real time data.

Occasionally, there may be errors in the LPR system's read of a license plate. Therefore, an alert alone shall not be a basis for police action (other than following the vehicle of interest). Prior to initiation of a stop of a vehicle or other intervention based on an alert, Department members shall undertake the following:

(2) Department members will document all stops from hot list alerts by indicating the positive ALPR Hit, i.e., with an arrest or other enforcement action on a computer generated spreadsheet that shall include at minimum a) the Department member's name that responded to the alert, b) the justification for responding to the alert, c) the related case number, d) the disposition code, e) time and date of the response, and f) and any known next steps or follow up (e.g. forwarding case to District Attorney, alerting owner to recovered stolen vehicle).

(B) **Database Investigative Queries**: Historical searches of scanned plates is permissible solely for missing or at-risk persons, witness locates, violent crime investigation, and in response to any subpoena, warrant, or other court order. Accessing the data shall be based on a standard of Reasonable Suspicion or greater.

For each query, the Department shall record (1) the date and time the information is accessed, (2) the license plate number or other data elements used to query the ALPR system, (3) the username of the person who accesses the information, and, as applicable, the organization or entity with whom the person is affiliated, and (4) the purpose for accessing the information. These records shall be attached to the annual report required by O.M.C. 9.64 et seq.

1. General Hot Lists (such as SVS and NCIC) will be automatically downloaded into the ALPR system a minimum of once a day with the most current data overwriting the old data.

2. All entries and updates of specific Hot Lists within the ALPR system will be documented by the requesting Department member within the appropriate general offense report. All entries shall be approved by the ALPR Administrator (or his/her designee) before initial entry within the ALPR system. The hits from these data sources should be viewed as informational; created solely to bring the officers attention to specific vehicles of interest that might have been associated with criminal activity.

   All Hot Plates and suspect information entered into the ALPR system will contain the following information as a minimum:

- Entering Department member's name
- Related case number
- Justification for entering the plate and/or other identifying information

onto the Hot List.

- Date and time of entry

3. Restrictions on Use

Permitted/Impermissible Uses. The ALPR system, and all data collected, is the property of the Oakland Police Department. Department personnel may only access and use the ALPR system consistent with this Policy. The following uses of the ALPR system are specifically prohibited:

(1) Invasion of Privacy: Except when done pursuant to a court order such as a search warrant, it is a violation of this Policy to utilize the ALPR to record license plates except those of vehicles that are exposed to public view (e.g., vehicles on a public road or street, or that are on private property but whose license plate(s) are visible from a public road, street, or a place to which members of the public have access, such as the parking lot of a shop or other business establishment). OPD shall make reasonable efforts to restrict the usage of the ALPR technology to the public right of way and other public property in alignment with this restriction.

(2) Harassment or Intimidation: It is a violation of this Policy to use the ALPR system to harass and/or intimidate any individual or group.

(3) Use Based on a Protected Characteristic. It is a violation of this policy to use the ALPR system or associated scan files or hot lists solely because of a person's, or group's race, gender, religion, political affiliation, nationality, ethnicity, sexual orientation, disability, or other classification protected by law.

(4) Personal Use: It is a violation of this Policy to use the ALPR system or associated scan files or hot lists for any personal purpose.

(5) First Amendment Rights. It is a violation of this policy to use the ALPR system or associated scan files or hot lists for the purpose or known effect of infringing upon First Amendment rights.

No data from ALPR shall be used or shared with other agencies for the purpose of pursuing criminal charges or civil enforcement against individuals for obtaining, providing, or supporting reproductive health care services, to ensure that medical rights of residents of and visitors to Oakland, a Sanctuary City, remain intact.

Department members shall not use, or allow others to use, the equipment or database records for any unauthorized purpose (Civil Code §798.90.51.; Civil Code § 1798.90.53).

a. No member of this department shall operate ALPR equipment or

access ALPR data without first completing department-approved training.

b. No ALPR operator may access department, state or federal data unless otherwise authorized to do so pursuant to Section E "Data Access" below.

c. Accessing data collected by ALPR requires a right to know and a need to know. A right to know is the legal authority to receive information pursuant to a state or federal statute, applicable case law, or a court order. A need to know is a compelling reason to request information such as involvement in an active investigation.

D. Data Collection: *The information that can be collected by the surveillance technology. Where applicable, list any data sources the technology will rely upon, including "open source" data.*

ALPR technology works by automatically scanning license plates on vehicles that are publicly visible. ALPR reads these license plates, compares the license plate characters (as well as vehicle attributes such as vehicle color or make and model with some ALPR systems) against specific databases, and stores the characters along with the date, time, and location where the photograph was taken, in a database.

E. Data Access: *The category of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information.*

Department sworn personnel, police service technicians, or other authorized Department personnel may use the technology. Authorized users other than sworn personnel or police services technicians (PST) must be designated by the Chief of Police or designee.

Data may not be shared with out of state or federal agencies, per California law.

The Oakland Police Department does not permit the sharing of ALPR data gathered by the city or its contractors/subcontractors for purpose of federal immigration enforcement, pursuant to the California Values Act (Government Code § 7282.5; Government Code § 7284.2 et seq) – these federal immigration agencies include Immigration and Customs Enforcement (ICE) and Customs and Border Patrol (CPB).

All data and images gathered by the ALPR are for the official use of this department. Some information may not be disclosable to the general public. Investigatory records are not generally disclosable in response to a public records request. Non-investigatory records shall be disclosed in response to a public records request.

F. Data Protection: *The safeguards that protect information from unauthorized access, including encryption and access control mechanisms.*

All data shall be safeguarded and protected by both procedural and technological means. OPD shall observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

1. All ALPR server data shall be accessible only through a login/password-protected system capable of documenting all access of information by username, license number or other data elements used in the search, name, date, time and purpose. (Civil Code § 1798.90.52).

2. Data will be transferred from LPRs to the designated storage per the ALPR technology data transfer protocol.

G. Data Retention: *The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period.*

All ALPR data uploaded to the server shall be purged from the server at the point of six (6) months from initial upload. ALPR information may be retained outside this retention limit solely for the following purposes:

1. Active Criminal Investigations

2. Missing or at-risk Persons Investigations

3. Investigations from other law enforcement or prosecutorial agencies where there is a legal obligation to retain information.

H. Public Access: *how collected information can be accessed or used by members of the public, including criminal defendants.*

Requests for ALPR information by non-law enforcement or non-prosecutorial agencies will be processed in accordance with Civil Code § 1798.90.55, Government Code §6253 et seq, this policy, and applicable case law and court orders.

I. Third Party Data Sharing: *If and how other City departments, bureaus, divisions, or non-City entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information.*

ALPR server data may be shared only as otherwise permitted by law and this policy. All data and images gathered by the ALPR are for the official use of this Department.

OPD personnel may share ALPR server data when there is a legal obligation to do so, such as a subpoena, court order or warrant to share such information, such as the following:

- a District Attorney's Office for use as evidence to aid in prosecution, in accordance with laws governing evidence;

- a Public Defender's Office or criminal defense attorney via the District Attorney's Office in accordance with applicable California criminal discovery laws;
- California law enforcement agencies as part of a formal criminal or administrative investigation;
- a party to civil litigation, or other third parties, in response to a valid court order only.

When there is no legal obligation to provide the requested data, requests for ALPR server data from other California law enforcement agencies shall be made in writing and may only be approved by the BOS deputy director or designee per the protocol below. These requests shall be maintained in a secure folder so that information about these requests can be shared in required annual reports with the PAC. Server access shall be restricted only to authorized OPD personnel who will extract the required information and forward it to the requester.

1. The requesting party shall have a right to know, and a need to know. A right to know is the legal authority to receive information pursuant to a court order, statutory law, case law, or sworn officer status. A need to know is a compelling reason to request information such as direct involvement in an investigation.

2. The Department shall record the requesting party's name and document the right and need to know the requested information.

3. The Department shall record whether the request was honored or denied, the reason for such action, and the name of the Department officer that processed the request.

J. Training: *The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology.*

The Training Section shall ensure that members receive department-approved training for those authorized to use or access the ALPR system and shall maintain a record of all completed trainings. (Civil Code § 1798.90.51; Civil Code §1798.90.53).

Training requirements for employees shall include the following:

- Applicable federal and state law
- Applicable policy
- Functionality of equipment
- Accessing data
- Safeguarding password information and data
- Sharing of data
- Reporting breaches
- Implementing post-breach procedures

K. ***Auditing and Oversight:*** *The mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy.*

Login/Log-Out Procedure. To ensure proper operation and facilitate oversight of the ALPR system, all users will be required to have individual credentials for access and use of the systems and/or data, which has the ability to be fully audited. It is the responsibility of the Department under this policy to actively pursue software and hardware upgrades that are needed to maintain full compliance with Section K of the use policy.

The records of Database Investigatory Queries, Third Party Data Sharing, and Hot List entries shall be incorporated into the annual report required by O.M.C. 9.64 et seq.

ALPR system audits shall be conducted annually to ensure proper system functionality and that personnel are using the system according to policy rules via sample audits, and reviews of training records.

OPD shall provide the Privacy Advisory Commission and the City Council's Public Safety Committee with quarterly reports regarding the efficacy of ALPR, to include at minimum the following information:

(a) Case number;

(b) Date and time that the incident was reported to OPD;

(c) Justification for the database query;

(d) Date of any OPD action or response to the incident;

(e) Nature of the action or response; and

(f) Confirmation as to whether and how ALPR assisted in resolution of the incident.

L. ***Maintenance:*** *The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained.*

1. **ALPR Administration:** All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the BOS.

2. **ALPR Administrator:** The BOS Deputy Director shall be the administrator of the ALPR program, and shall be responsible for developing guidelines and procedures to comply with the requirements of Civil Code § 1798.90.5 et seq. The BOS Deputy Director is responsible for ensuring systems and processes are in place for the proper collection, and retention of ALPR data.

3. **ALPR Coordinator:** The title of the official custodian of the ALPR system is the ALPR Coordinator.
4. **Monitoring and Reporting:** The Oakland Police Department will ensure that the system is remains functional according to its intended use and monitor its use of ALPR technology to ensure the proper functionality of the system as defined in the policy guidelines of this document, including required audits, training, and data access records.
5. The ALPR Coordinator shall provide the Chief of Police, Privacy Advisory Commission, and Public Safety Committee with an annual report pursuant to OMC 9.64 (Oakland Surveillance Technology Ordinance).

By Order of

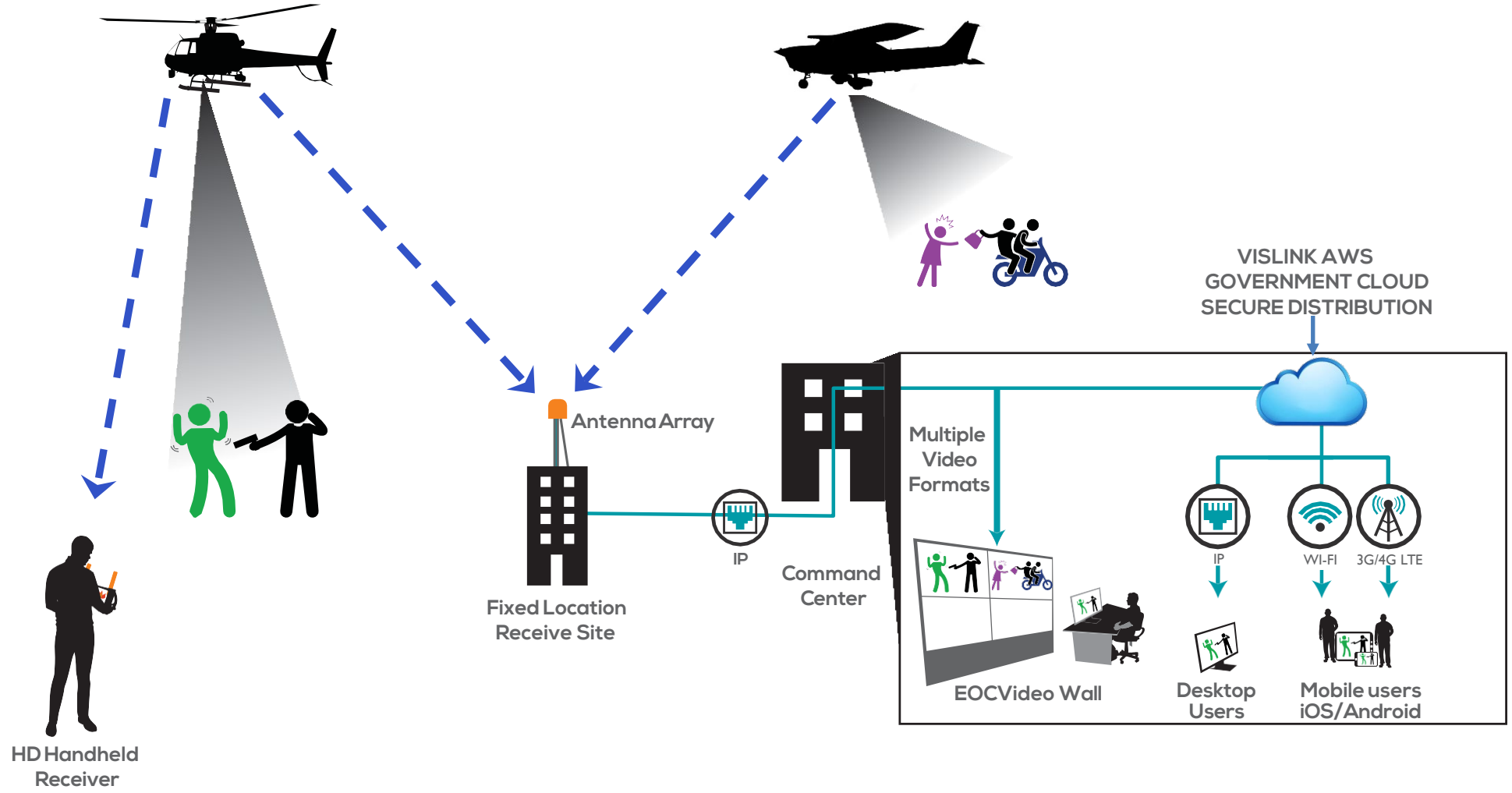
Darren Allison, Interim Chief of Police Date Signed:

VISLINK

Oakland Police Department

Airborne Surveillance Video Downlink

Fixed and Handheld Receive Solution



Oakland Police Department

Airborne Surveillance Video Downlink Solution

Vislink is proposing to provide the Oakland Police Department with a state-of-the-art airborne surveillance video downlink transmit & receive solution that will provide real-time, high quality high-definition airborne images from two aircraft, operating simultaneously, to both fixed and mobile ground receive units.

This high-quality encrypted/secure video downlink solution will provide real-time actionable video images to both command staff and remote users, allowing for critical decision making, enhancement of officer safety and better allocation of resources.

AIRCRAFT TRANSMIT SOLUTION

Vislink is proposing to provide a new AeroLink 6.5 GHz, high power, high definition, RF transmitter in the proposed Diamond DA62 aircraft platform. The Vislink AeroLink RF transmitter can provide up to 4K UHD encoding.

Vislink is proposing a low-cost and no maintenance omnidirectional antenna system for this aircraft, this antenna will be belly mounted. Utilizing a low-cost omnidirectional antenna allows the aircraft to transmit simultaneously to future multiple fixed receive sites, providing greater area coverage

and signal reliability, as well as to mobile command vehicles and hand-held tactical receive systems.

The Vislink RF transmit system will be fully controlled by the aircrafts mapping & navigation system, allowing for easier control by the Tactical Flight Officer.

FIXED RECEIVE & DISTRIBUTION SOLUTION

Vislink is proposing to provide and install a single 2-channel fixed receive site solution on the existing self-support tower structure or building structure within the City of Oakland. The proposed Vislink solution will allow any two aircraft to simultaneously transmit live video downlink images, into the fixed receive system.

The proposed fixed tower solution receives the aircraft signals and then provides an IP output stream, which is then transported over the cities secure data network to the Police EOC facility, where the actionable video images it can be viewed by command staff on a video wall or dedicated television monitor.

Additionally, Vislink will provide a secure cloud distribution and viewing system, no video recording or storage will be provided. The downlink images will be sent to an AWS Government Cloud instance, where the video can be observed by only authorized users, via password protection.

This solution allows for a hands-off viewer approach, allowing command staff access to actionable video images, without he need to initiate the downlink reception from the command center.

PORTABLE / TACTICAL HAND-HELD RECEIVE SOLUTION

Vislink will also provide one of our MobilCMDR portable / tactical hand-held receive kits. This self-contained hand-held receiver allows for direct viewing of encrypted aircraft video downlink images on a daylight viewable screen, as well as connection to an external monitor via a coax cable connection.

This unit can also be utilized at the police aviation hangar to test the aircraft transmit system, to ensure proper operation prior to flight.

CITY OF OAKLAND

MEMORANDUM

TO:	Darren Allison, Interim Chief of Police	**FROM:**	Drennon Lindsey, Deputy Chief OPD, Bureau of Investigations
SUBJECT:	Forensic Logic CopLink System – 2022 Annual Report	**DATE:**	June 29, 2023

Background

Oakland Municipal Code (OMC) 9.64.040: Surveillance Technology "Oversight following City Council approval" requires that for each approved surveillance technology item, city staff must present a written annual surveillance report for Privacy Advisory Commission (PAC). After review by the PAC, city staff shall submit the annual surveillance report to the City Council. The PAC shall recommend to the City Council that:

- The benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded.
- That use of the surveillance technology cease; or
- Propose modifications to the corresponding surveillance use policy that will resolve the concerns.

Oakland Police Department (OPD) Department General Order (DGO) I-24: Forensic Logic CopLink, as well as OMC 9.64.040 together require that OPD provide an annual report to the Chief of Police, the PAC, and Public Safety Committee. The information provided below is compliant with these annual report requirements.

DGO I-24 explains that authorized members may use CopLink for the purpose of searching the system in the service of conducting criminal investigations, such as apprehending subjects, locating and returning stolen property, as well as in the protection of the law enforcement officers encountering the individuals described in the system. Authorized purposes also include other appropriate OPD organizational investigations (e.g., internal affairs, missing persons, and use of force investigations).

Captain David Elzey, Criminal Investigation Division Commander, was the Program Coordinator for 2022.

A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

Forensic Logic search technology is used regularly by both OPD sworn field / patrol personnel and command staff. Search parameters include the following criteria which are submitted to a search engine where data originating from law enforcement records, calls for service, field interviews, arrest/booking records and citations are stored:

- *License plate numbers*
- *Persons of interest*
- *Locations*
- *Vehicle descriptions*
- *Incident numbers*
- *Offense descriptions/penal codes*
- *Geographic regions (e.g., Police Beats or Police Areas)*

Data is stored in an FBI Criminal Justice Information Service (CJIS) compliant repository in the Microsoft Azure GovCloud and encryption of data both at rest and in transit is protected by being compliant with FIPS 140-2.

In 2022, there were a total of 550 distinct users who conducted Forensic Logic searches, for a total of 398,386 separate queries. Table 1 below breaks down this search data by month and by distinct user and total searches.

Table 1: OPD CopLink Searches; by Distinct User and Search Totals – 2022

Search Type	***January***	***February***	***March***	***April***	***May***	***June***
Number of OPD distinct users in each month	*306*	*316*	*330*	*299*	*297*	*311*
Number of searches conducted	*37,257*	*30,699*	*41,585*	*33,084*	*32,054*	*34,658*

Search Type	***July***	***August***	***September***	***October***	***November***	***December***
Number of OPD distinct users in each month	*300*	*297*	*324*	*328*	*315*	*309*
Number of searches conducted	*32,404*	*32,823*	*32,896*	*30,410*	*30,250*	*30,266*

B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

Data searched with the Forensic Logic CopLink system is entirely acquired from incident reports, citations, calls for service and field interviews that have already been recorded in originating Records Management Systems, Computer Aided Dispatch Systems, and Mobile Field Reporting Systems – from both OPD systems as well as from other law enforcement agency systems (other Forensic Logic client agencies). The data is collected from OPD systems at least once every 24 hours; once the data is collected and resides in the Forensic Logic cloud repository, it is made available to agencies subscribing to the Forensic Logic service who are permitted by their agency command staff to access CJIS information.

This is the warning message on the service user sign-on page that every user sees prior to accessing the system:

WARNING: You are accessing sensitive information including criminal records and related data governed by the FBI's Criminal Justice Information System (CJIS) Security Policy. Use of this network provides us with your consent to monitor, record, and audit all network activity. Any misuse

of this network and its data is subject to administrative and/or criminal charges. CJIS Security Policy does not allow the sharing of access or passwords to the Forensic Logic Coplink Network™. The data content of the Forensic Logic Coplink Network™ will not be considered for use as definitive probable cause for purposes of arrests, searches, seizures or any activity that would directly result in providing sworn testimony in any court by any participating agency. Information available in the Forensic Logic Coplink Network™ is not probable cause, but indicates that data, a report or other information exists in the Records Management System or other law enforcement, judicial or other information system of an identified participating agency or business.

In accordance with California Senate Bill 54, applicable federal, state or local law enforcement agencies shall not use any non-criminal history information contained within this database for immigration enforcement purposes. This restriction does not pertain to any information that is regarding a person's immigration or citizenship status pursuant to 8 U.S.C. §§ 1373 and 1644.

Data sourced from the Oakland Police Department cannot be accessed by US DHS ICE nor US DHS CBP staff.

C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to.

The CopLink service is accessible by authorized OPD users on OPD computers with an appropriate user-id and password (criteria for both defined by FBI CJIS Security Addendum). OPD data sources that provide data accessible to the search tool include the following:

- *Arrest records*
- *Field contacts*
- *Incident reports*
- *Service calls*
- *Shots fired (ShotSpotter)*
- *Stop Data reports*
- *Traffic Accident reports*

D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year:

CopLink software is not deployed in a manner as is physical hardware technology. The software is used by OPD personnel at the Police Administration Building, Eastmont Building, Communications Center, the Emergency Operations Center (when active), and in patrol vehicles to search crime incidents and related data. The data itself can relate to crime data with geographic connections to anywhere in the City, as well as the broader region and even nationally.

E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The PAC may waive this requirement upon making a

determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the PAC makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review.

Staff reached out to each City Council office to ask about possible community complaints or concerns related to this surveillance technology. No community complaints or concerns were communicated to staff.

OPD is not able to provide the race of each person connected to each CopLink query. There are thousands of queries and not all queries would provide race data of each suspect or person connected to each data result. Staff therefore recommend that the PAC makes the determination that the administrative burden in collecting or verifying this information as well as the associated potential for greater invasiveness in capturing such data outweighs the public benefit.

F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information:

Forensic Logic conducted an audit of OPD system queries to ensure all logins were conducted by existing OPD personnel.

Forensic Logic is notified of additions or deletions to its subscription services by the designated Point of Contact at the OPD. Forensic Logic also would modify the user census upon the request of any Chief of Police, Assistant Chief of Police or Deputy Chief of Police of the OPD.

In addition, all OPD users can only use Forensic Logic services from within OPD designated facilities such as the Police Administration Building, the Eastmont Building, the Communications Center, the Emergency Operations Center (when active), and from inside a patrol vehicle due to Forensic Logic's requirement that Internet Protocol (IP) addresses for users be whitelisted (be enabled for access). Any attempt to login to the Forensic Logic services outside of those locations would fail by any person with an authorized OPD user id (email address).

In addition, on an annual basis, Forensic Logic will prepare a list of enabled OPD users for review by the OPD Point of Contact to confirm that all users should be enabled for access to the Forensic Logic services. Should individuals need to be removed from the services, the Point of Contact will notify Forensic Logic at that time.

G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response.

There were no identifiable data breaches or unauthorized access during the year of 2022.

H. Information, including case examples, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes:

Armed Robbery Series Targeting Construction Workers and Their Tools

Starting in July 2022, multiple suspects were involved in an armed robbery series where the targeted victims were construction workers and their power tools. During the investigation, the assigned Robbery Unit investigator identified one suspect. The investigator conducted a LEAP/CopLink search of the suspect's name, and several crime reports/field contact reports were located showing the suspect's previous contacts. The suspect was listed in an Oakland Police crime report as a shooting victim in 2021. A cell phone number for the then shooting victim (suspect) was listed in the crime report. A separate field contact report for the suspect listed the same cell phone number. The investigator obtained a cell phone ping warrant for the listed cell phone number associated with the suspect. The information gleaned from the cell phone ping warrant assisted in tracking the suspect and placing him on scene of two of the robberies.

There was an identified vehicle used by the suspects in their robberies. The investigator conducted a LEAP/CopLink search on the vehicle's license plate and discovered it was associated to another suspect based on a stop data information in LEAP/CopLink. The investigator consequently connected this suspect to the suspect vehicle and one of the robbery incidents.

Home Invasion Robbery

In February 2022, three suspects committed a home invasion armed robbery. The suspects forced entry into a home, assaulted a victim, and stole property and cash. The case was assigned to a Robbery Investigator. During the investigation, one suspect (S-1) was identified by name. The investigator conducted a LEAP/CopLink search on the suspect which revealed several field contact reports where the suspect (S-1) was associated with a male subject who matched the description of one of the other suspects (S-3) provided by the victim. The investigator conducted a LEAP/CopLink search on S-3 which revealed several recent contacts throughout Alameda County where he was in a vehicle; the vehicle noted in these contacts matched the suspect vehicle that was observed on surveillance cameras at the time the home invasion robbery occurred. The victim subsequently identified S-1 and S-3 in a photo lineup. The investigator obtained arrest warrants for S-1 and S-3, and they were taken into custody.

Armed Robbery

In December 2022, three suspects committed an armed robbery of two victims. The case was assigned to a Robbery Investigator. During the investigation, it was discovered that a credit card belonging to one of the victims was used at a liquor store in Oakland. The investigator reviewed surveillance video from the liquor store capturing the date/time the stolen credit card was used. From the liquor store surveillance video, the investigator observed subjects using the stolen credit card and then enter a vehicle. The investigator conducted a LEAP/CopLink search on the vehicle which led to the identification of one of the suspects. The LEAP/CopLink search provided information on the registered owner of the vehicle in addition to who was previously contacted operating the vehicle. Based on previous contact information involving the vehicle, the investigator connected one of those individuals as being one of the suspects involved in the robbery. The investigator subsequently obtained an arrest warrant for this suspect.

I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates:

There are no existing or newly opened public records requests relating to Forensic Logic, CopLink, or LEAP (former name for CopLink).

J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year:

Tables 2 and 3 below provide costing data from the current Oakland Forensic Logic contract.

Table 2: Oakland Forensic Logic Contract Cost; July 2020 – June 2022

For the Period 07/01/2020 through 06/30/2022 payable upon execution of agreement:

Product Number	Description	List Price	Sales Price	Quantity	Subtotal	Discount (%)	Total Price
	CopLink SEARCH (07/01/20-06/30/21)	$275	$199	794	$158,006	0%	$158,006
	CopLink Analytics (07/01/20-06/30/21)	$1,000	$1,000	794	$794,000	100%	$0
	CopLink CONNECT (2 Years)	$20,000	$20,000	1	$20,000	0%	$20,000
	Integration Services NIBIN	$5,000	$5,000	1	$5,000	0%	$5,000
	Integration Services Motorola Premiere One CAD and RMS	$25,000	$25,000	1	$25,000	0%	$25,000
	CopLinkX (07/01/21-06/30/22)	$275	$275	794	$218,350	0%	$218,350
	Integration and Maintenance Services	$25,000	$25,000	1	$25,000	0%	$25,000
	Round down discount		($356)	1	($356)		($356)
						TOTAL	$451,000

Table 3: Oakland Forensic Logic Contract Cost; July 2022 – June 2023

For the Period 07/01/2022 through 06/30/2023 payable on July 1 2021:

Product Number	Description	List Price	Sales Price	Quantity	Subtotal	Discount (%)	Total Price
	CopLink SEARCH						
	CopLink Analytics						
	CopLink CONNECT	$10,000	$10,000	1	$10,000	0%	$10,000
	CopLinkX	$275	$275	794	$218,350	0%	$218,350
	Integration and Maintenance Services	$25,000	$25,000	1	$25,000	0%	$25,000
	Round down discount		($350)	1	($350)		($350)
						TOTAL	$253,000

K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request:

No requests for changes at this time.

OPD is committed to providing the best services to our community while being transparent and instilling procedural justice through daily police activity. This report is in compliance with these OPD commitments. OPD hopes that this report helps to strengthen our trust within the Oakland community.

Respectfully submitted,

_____

Drennon Lindsey, Deputy Chief of Police
OPD, Bureau of Investigations

Reviewed by:
David Elzey, Captain of Police
OPD, Criminal Investigation Division

Prepared by:
Tracey Jones, Police Services Manager
OPD, Research and Planning Unit

L3HARRIS™
FAST. FORWARD.

WESCAM MX™-15.
FULLY DIGITAL. HIGH DEFINITION.

A Multi-Sensor, Multi-Spectral Imaging System in a Single Line Replaceable Unit (LRU)

ACTIONABLE INTELLIGENCE

The WESCAM MX-15 is ideal for medium-altitude, covert ISR, SAR missions and homeland security.

MULTI-SENSOR IMAGING/LASING PAYLOAD OPTIONS

- Supports seven payload items simultaneously
- HD thermal, HD daylight and HD low-light and HD SWIR cameras provide 24/7 imaging
- Continuous wide-angle zoom
- High-magnification step-zoom spotter
- High-sensitivity color low-light imaging
- Eye-safe laser rangefinder[1]
- Laser illuminator[2] in choice of wide, narrow or ultra narrow divergence

HIGH-PERFORMANCE GIMBAL

- 4-axis stabilized turret with internal passive isolator for excellent stabilization performance
- Sharp optics and superior stabilization performance results in industry leading target detection, recognition and identification range performance in the 15” class
- Inertial Measurement Unit (IMU) mounted to optical bench for high target location accuracy
- Inertial Navigation System (INS) auto-align to aircraft

ADVANCED IMAGE PROCESSING

- Real-time image enhancement on all sensors
  - High-performance haze penetration
  - Improved feature recognition and ID
  - 2x, 4x Ezoom
  - Advanced video tracker
  - Imaging blending
  - Embedded Moving Target Indication
  - Pseudo-color IR

WESCAM ADVANCED VIDEO ENGINE (WAVE)

- A high-performing embedded computing engine engineered to support advanced image-processing capabilities
- WAVE architecture includes a state-of-the-art graphics processing unit (GPU) - enabling future advancements in image processing & surveillance automation

L3Harris.com

INTERFACE FLEXIBILITY

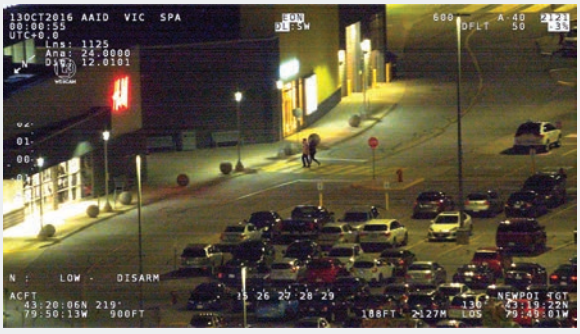
- Built-in video switch matrix provides multiple HD-SDI and analog video outputs
- 720p or 1080p HD video
- Wide range of data ports: RS-232/422, Ethernet, MIL-STD-1553B, ARINC429
- All standard WESCAM MX-Series functional interfaces

RUGGEDNESS

- Rugged aerospace grade aluminum structure
- MilSpec environmental, EMC, and power quality qualification
- Built-in vibration isolator protects internal payload components
- Rigorous environmental stress screening (ESS)
- Designed to minimize maintenance requirements and simplify repair

SIMPLIFIED AIRCRAFT INTEGRATION

- Electronics unit inside the turret
- Built-in vibration isolation
- Built-in GPS receiver
- <19” turret height for better ground clearance
- Compatible with standard quick disconnect mounts
- Side mounted connectors for recessed installations
- No calibration required for LRU swapout



WESCAM MX-15

[1]Consult factory for specific environmental and target conditions

[2]

L3HARRIS™
FAST. FORWARD.

1025 W. NASA Boulevard
Melbourne, FL 32919
t 1 800 668 4355
info.wescam@L3Harris.com

L3HARRIS™
FAST. FORWARD.

WESCAM MX™-15.
FULLY DIGITAL. HIGH DEFINITION.

PAYLOAD SPECIFICATIONS	
Sensor Options for Thermal Imager (Select #1a or #1b)	
Sensor #1a - Thermal Imager:	
Type:	MWIR, cooled
Resolution:	640 x 512 Pixels
Fields-of-View:	26.7° to 0.54°
Sensor #1b - HD Thermal Imager:	
Type:	MWIR, cooled
Resolution:	1280 x 1024 Pixels
Fields-of-View:	35.5° to 1.2°
Sensor #2 - HD Daylight Zoom:	
Type:	Color
Resolution:	1920 x 1080 Pixels
Fields-of-View:	31.2° to 1.2° - 720p, 31.2° to 1.8° - 1080p
Sensor Options for Low-Light Continuous Zoom and SWIR Continuous Zoom (Select #3a or #3b)	
Sensor #3a - Low-Light Continuous Zoom:	
Fields-of-View:	40.8° to 2.4°
Sensor #3b - SWIR Imager Continuous Zoom:	
Fields-of-View:	40.8° to 2.4°
Sensor #4 - HD Daylight Spotter:	
Type:	Color
Resolution:	1920 x 1080 Pixels
Fields-of-View:	0.72° to 0.29° - 720p, 1.1° to 0.43° - 1080p
Sensor Options for MX-Day/Night Spotter (Select #5a or #5b)	
Sensor #5a - HD Low-Light Spotter: (Used with Sensor #4)	
Resolution:	1920 x 1080 Pixels
Fields-of-View:	0.72° to 0.29° - 720p, 1.1° to 0.43° - 1080p
Sensor #5b - HD SWIR Spotter: (Used with Sensor #4)	
Sensor #6 - Laser Illuminator (LI)[1]:	
Wavelength:	860nm (near IR)
Beam Power:	700mW
Beam Divergence:	Wide, Narrow or Ultra Narrow
Sensor #7 - Secondary Laser Illuminator (LI)[1]:	
Wavelength:	860nm (near IR)
Beam Power:	150mW
Beam Divergence:	Narrow
Sensor #8 - Laser Rangefinder[2]	
Wavelength:	1.54µm
Range:	20km
Additional WESCAM MX-15 Features and Embedded Options:	
> Optical Bench IMU > AutoTracker > GPS Receiver	> Moving Target Indicator > LDDT (SWIR tracking of multiple 3rd party designator spots)
Notes:	All FOVs are for digital outputs: Consult factory for FOVs for analog outputs up to 4x Ezoom available.

TURRET SPECIFICATIONS	
Stabilization and Steering	(4) Axis + (6) DoF Isolator Azimuth Range: Continuous 360° Elevation Range: +90° to -120°

SYSTEM SPECIFICATIONS	
WESCAM MX-15 Turret	<95 lbs / 43.2 Kg (all sensors), 15.5”(D) x 18.95”(H), 393.7mm (D) x 481.33mm (H)
Power	MIL-STD-704F, 280W (Avg.)

FEATURES AND BENEFITS

- > Multi-Sensor Imaging/Lasing Payload Options
- > Short-Wave Infrared (SWIR) Imaging
- > High-Performance Gimbal
- > Advanced Image Processing
- > Interface Flexibility
- > Ruggedness
- > Simplified Aircraft Integration

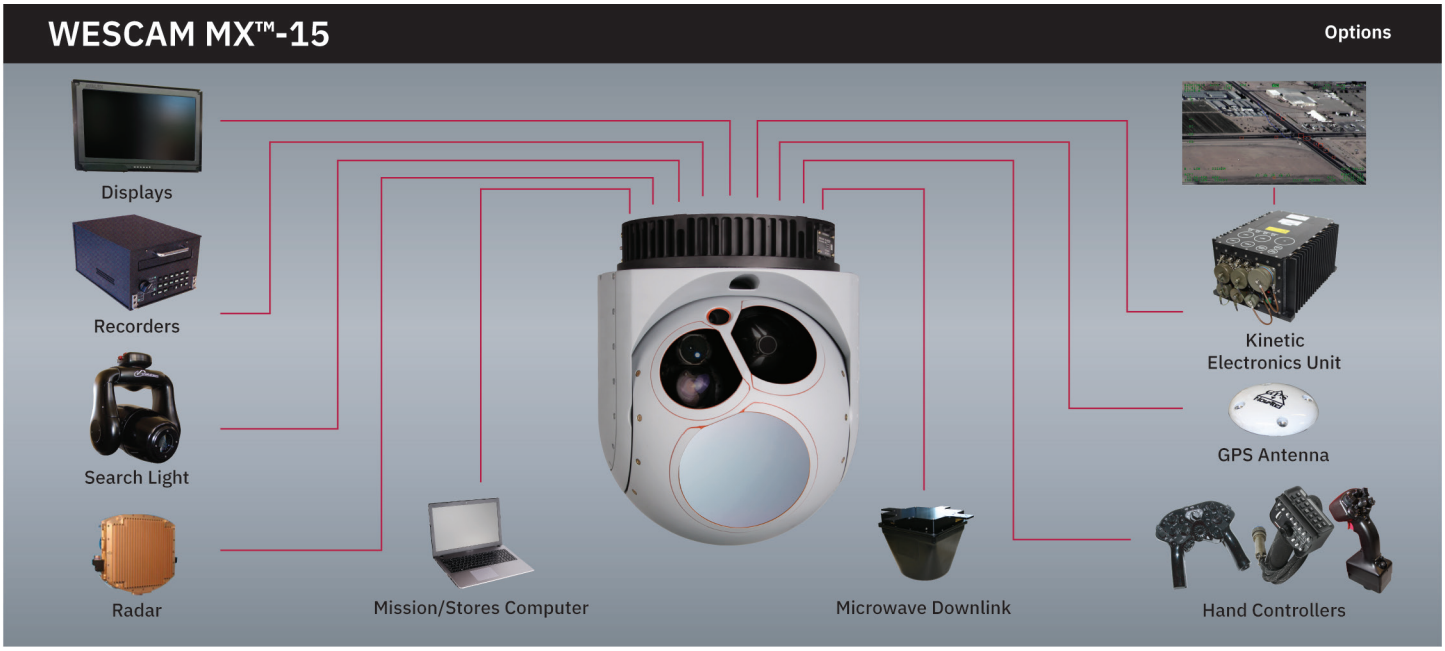
L3Harris.com

The WESCAM MX-15 is an advanced, industry-leading stabilized multi-sensor, multi-spectral imaging system that is renowned for high performance, operator ease-of-use, and reliability. It's ideal for a wide range of missions, including medium altitude covert intelligence, surveillance, and reconnaissance, armed reconnaissance, search and rescue. The system provides imagers for optimal performance in a wide range of conditions; bright sunlight, overcast/dusk, smoke, and complete darkness. That is supported by a suite of advanced image processing algorithms for noise reduction, sharpening, and local area contrast enhancement that aid feature recognition.

Superior stabilization is the key to achieving the maximum target detection, recognition, and identification range performance from the imagers. The WESCAM MX-15 achieves this with a hybrid active and passive jitter suppression system. This proven architecture stabilizes all devices on the optical bench equally. In addition, stable and accurate target geolocation ensures that the crosshairs stay on a stationary target, regardless of changes to aircraft position, attitude, and heading. This significantly reduces the operator burden in keeping eyes on target.

Advanced processing features such as object tracking, image blending, and moving target indication further serve to automate the search and tracking process, allowing the operator to focus on the target versus the equipment.

To ensure that the WESCAM MX-15 is fit for the mission, it is fully qualified to MIL-STD-810 for environmental withstanding, MILSTD-461 for electromagnetic compatibility, and MIL-STD-704 for power quality.



VIDEO INTERFACES
Built-in video switch matrix
6 independent HD-SDI output channels available
5 analog video (NTSC or PAL) output channels available

DATA INTERFACES
Interface Types: RS-232/422, Ethernet, MIL-STD-1553B, ARINC 429
Functional Interfaces: Aircraft GPS/INS, Remote Control, Moving Map, Microwave / Data Link, Searchlight, Radar, Metadata / Status
HMI Options: Moving Map, Mission Console
Compatible with WESCAM Microwave Communications Equipment.

WESCAM MX-15

[1] [2] Consult factory for specific environmental and target conditions

L3HARRIS™
FAST. FORWARD.

1025 W. NASA Boulevard
Melbourne, FL 32919
t 1 800 668 4355
info.wescam@L3Harris.com

15 May 2023

Brandon Mart
Oakland Police Department
Air Support Unit

Subject: L3 Harris WESCAM MX-15 Performance

Brandon,

Per our discussion last week, I wanted to provide you with additional information on the performance of the MX-15. The L3 Harris WESCAM MX-15 does not contain or utilize any type of facial recognition software for the identification of subjects. The MX-15 does not utilize any type of artificial intelligence to assist in the identification of subjects.

The industry standard for evaluating imaging performance is Detection, Recognition, and Identification ranges. This criterion was developed for the identification of standard military vehicles and does not necessarily represent the ability distinguish person A from person B in the case of a human target. Range performance is dependent on a variety of factors including altitude, atmospheric conditions, and target characteristics at the time of flight. The values provided here are for 23 km Visibility and 5,000 ft altitude above ground level.

Human Target (0.5 m x 1.5 m)

Electro-Optical Narrow (EON) Spotter (Daylight/Color Imager) 1500 mm Focal Length
Detection 36 km
Recognition 22 km
Identification 7.5 km

Infrared Imager 880 mm Focal Length
Detection 19.2 km
Recognition 10.7 km
Identification 3.9 km

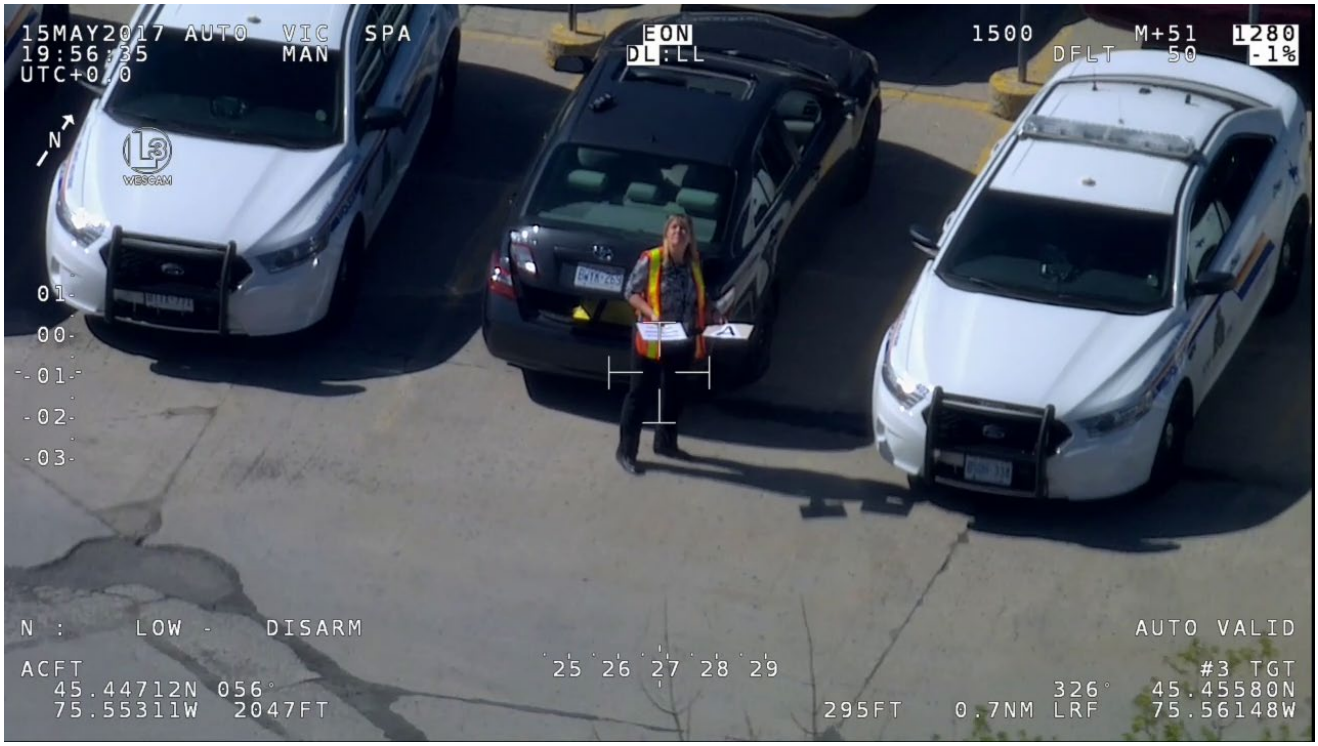
The identification at these ranges will not provide enough information to specifically identify a particular person. At most it will provide general description.

The Mid-Wave Infrared sensor will not see through wall or other solid structures and as a rule will not see through glass or other thermal barriers.

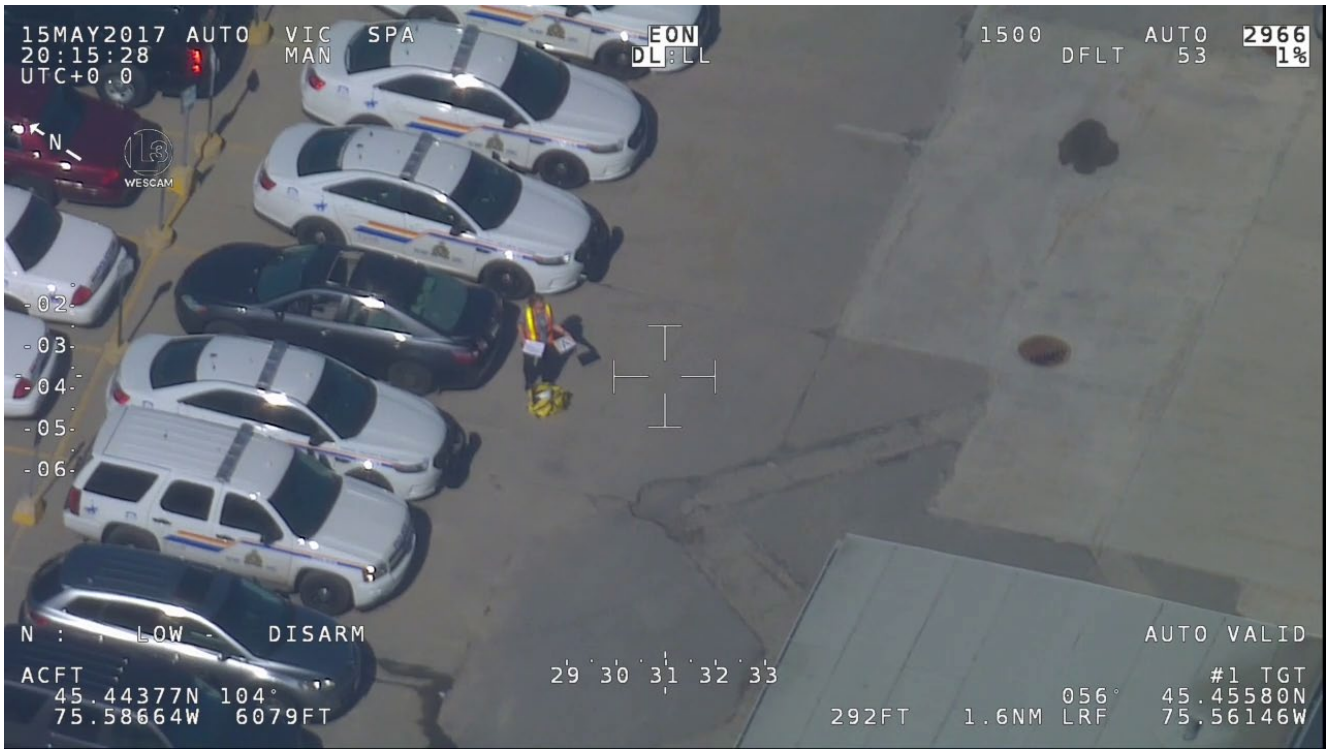
I have included several frame captures from MX-15 video to help provide additional clarity on the MX-15 performance capabilities. The images were taken during different evaluation flights, some at different locations and on different days.

Please let me know if you have questions or need additional information.

Ken Scarboro
Principal, Business Development
L3Harris Wescam USA
707-477-0128
Ken.Scarboro@L3Harris.com



MX-15 from 2,000 ft altitude .7nm (1.3 km) slant range EON 1500 mm



MX-15 from 6000 ft altitude 1.6 nm (3 km) slant range EON

MX-15 from 6000 ft 3.4 km (1.8 nm) slant range EON

MX-15 from 6,000 ft 4.3 km (2.3 nm) EON

MX-15 from 2,000 ft 1.5 km slant range (.8 nm) IR

CITY OF OAKLAND

MEMORANDUM

TO: Darren Allison, Interim Chief of Police

FROM: Trevelyon Jones, Captain, Ceasefire Section

SUBJECT: Gunshot Location Detection System (ShotSpotter) – 2022 Annual Report

DATE: June 23, 2023

Background

Oakland Municipal Code (OMC) 9.64.040: Surveillance Technology "Oversight following City Council approval" requires that for each approved surveillance technology item, city staff must present a written annual surveillance report for Privacy Advisory Commission (PAC). After review by the Privacy Advisory Commission, city staff shall submit the annual surveillance report to the City Council. The PAC shall recommend to the City Council that:

- The benefits to the community of the surveillance technology outweigh the costs and that civil liberties and civil rights are safeguarded.
- That use of the surveillance technology cease; or
- Propose modifications to the corresponding surveillance use policy that will resolve the concerns.

The PAC recommended adoption of OPD Department General Order (DGO) I-20: "Gunshot Location Detection System" at their October 3, 2019, meeting; the report was presented to the City Council on November 19, 2019, and adopted by the City Council via Resolution No. 87937 C.M.S. DGO I-20 requires that OPD provide an annual report to the Chief of Police, the Privacy Advisory Commission (PAC), and the City Council.

2022 Data Details

A. A description of how the surveillance technology was used, including the type and quantity of data gathered or analyzed by the technology:

From the "Surveillance Impact Use Report for the Gunshot Location Detection System:"

Part 1 – How the System Works: "The GLD system sensors are designed to detect gunshots based on their acoustic signature (e.g., broad-frequency, impulsiveness and loudness). The utilization of multiple sensors at different distances from a gunshot sound allows the system not only to capture the sound but assign a probability that it is a gunshot and triangulate its precise location based on time difference of arrival. If the machine classifier in the "ShotSpotter Cloud" determines it is likely a gunshot based on computer-learning algorithms, the system will pull a short audio snippet from the sensors that detected it and send it to human analysts at the ShotSpotter Incident Review Center at its headquarters in Newark, CA. The analysts perform an auditory and visual assessment of the audio waveform to make a final determination as part of a two-phased classification process. If confirmed as a gunshot, an alert is published containing

information such as street address, number of rounds fired, and a short audio snippet of the gunfire event– all within 60 seconds of the trigger pull (29 seconds on average)."

From Section 2: Proposed Purpose: "The purpose of GLD is to enable OPD to provide a higher level of the service to the community related to shootings. The system detects, locates and alerts officers of virtually all gunshots in a coverage area in less than 60 seconds enabling officers to respond to and investigate gunshots incidents they would not have known about and to respond to them much more rapidly than waiting for a 911 call. Personnel can better respond to gunshot activity and respond to possible armed individuals as well as to possible gunshot victims through this important real-time data."

ShotSpotter technology was used in the following ways/with the following outcomes in 2022:

- The number of times ShotSpotter technology was requested: ShotSpotter alerted OPD to 7,562 unique gunshot incidents from January 1 – December 31, 2022. Of those alerts**, 7,481 (99%) were not called in by the community as a 415GS call type (shots fired),** and OPD would not have known about them nor have been able to respond in a timely fashion. This information is based on an analysis of calls within 15 minutes and 1,000 feet of a ShotSpotter alert.
- ShotSpotter led police to **199 shooting cases, 28 of which were Homicide and 171 were Assault with a Firearm.** OPD was able to provide and coordinate immediate emergency medical response on these shooting cases; OPD personnel believe that several of these victims survived the shootings specifically because of the quick response and subsequent medical attention. In some instances, OPD and medical response occurred within less than two minutes of the ShotSpotter activation. The ShotSpotter alert was within 10 minutes and 1,000 feet of the location where the victim was found. Furthermore, staff believe that there were many more cases where OPD responded to activations and found shooting victims – and where critical medical attention was provided. The 199 cases cited here (171 injury cases) are the ones where OPD and ShotSpotter staff can conclusively cite the response to the ShotSpotter activations.
- ShotSpotter activations led OPD to **162 cases where their vehicle and/or dwelling was hit by gunfire. Of these 162 cases, 71 victims were present but not hit by gunfire, and 91 were listed as victims because the property belonged to them.**
- 1,789 crime incident reports (24% of total activations)
  - 1,252 (70%) of these incidents resulted in OPD Crime Lab requests for further firearm forensic analysis.
- ShotSpotter provided the following additional reports in relation to specific ShotSpotter activations:
  - **Eleven detailed forensic reports**
  - **Court preparation for seven cases (*DA subpoenaed ShotSpotter for this information*)**
  - **Investigative Lead Summary 1,181**

B. Whether and how often data acquired through the use of the surveillance technology was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s):

The following agencies have been provided log-in access to the ShotSpotter System for ongoing usage and do not make written requests for access:

OPD and the Oakland Housing Authority Police Department entered into a Memorandum of Understanding (MOU) in 2012, following City Council approval, to fund the initial ShotSpotter program in areas of the City and near OHA buildings known for higher levels of gun shots. This MOU allows OPD to share access to the ShotSpotter cloud-based portal with OHA PD personnel (see **Attachment C**).

DGO I-20 Section B – 1. "Authorized Use" (From Use Policy Approved by City Council November 19, 2019) states:

The Chief of Police or designee shall provide necessary training and/or technical assistance for GLD usage. Only OPD personnel shall be granted access to OPD's GLD System. The GLD system shall only be used for locating gunshots. The system shall never be used to record human conversations except where such conversations are unintentionally recorded in connection with gunshot recordings.

DGO I-20 provides rules for sharing ShotSpotter System data with outside agencies. Section C–3 of DGO I-20: "GUNSHOT LOCATION DETECTION SYSTEM" – "Releasing or Sharing GLD System Data," states:

"GLD system data may be shared only with other law enforcement or prosecutorial agencies based on a need to know or a right to know, or as otherwise required by law, using the following procedures:

1. The agency makes a written request for the ShotSpotter data that includes:
    a. The name of the requesting agency.
    b. The name of the individual making the request.
    c. The need for obtaining the information.
2. The request is reviewed by the Bureau of Services Deputy Chief/ Deputy Director or designee and approved before the request is fulfilled.
3. The approved request is retained on file and shall be included in the annual report.

There were no outside agency ShotSpotter data requests for OPD in 2022.

OPD investigators in the Criminal Investigations Division and or other sections of OPD such as the Ceasefire Section and Violent Crime Operations Center regularly communicate with personnel from other law enforcement agencies on interjurisdictional investigations; these forms of collaboration may involve discussions related to shootings where OPD became informed from ShotSpotter activations. ShotSpotter activations many times may lead to evidence gathering (e.g., finding bullet casings); OPD may share information about evidence

(e.g., that bullet casings were found in a particular area at a particular time). For prosecutorial purposes, OPD investigators may provide ShotSpotter data to be included with the investigative criminal case packet as relevant evidence to the District Attorney's Office as part of the case charging process and/or discovery.

C. Where applicable, a breakdown of what physical objects the surveillance technology hardware was installed upon; using general descriptive terms so as not to reveal the specific location of such hardware; for surveillance technology software, a breakdown of what data sources the surveillance technology was applied to:

OPD has contracted with ShotSpotter to install GLD sensors in different areas (phases) in several parts of the city. The total coverage area for the current ShotSpotter system comprises 18.17 square miles or approximately 32 percent of the city land size (55.93). OPD has chosen to install the sensors in areas most prone to gunshots based upon historical data. Many areas in East and West Oakland now benefit from the GLD system.

Most sensors are placed approximately 30 feet above ground level to maximize sound triangulation to fixed structures (e.g., buildings); at this altitude, the sensors can only record limited street-level human voice sounds. Furthermore, ShotSpotter only retains the audio for one second prior to a gun shot, and one second after.

D. Where applicable, a breakdown of where the surveillance technology was deployed geographically, by each police area in the relevant year:

Attachment A to this report provides the geographic areas of the City of Oakland that comprise the three ShotSpotter "phases" or areas covered under the current OPD-ShotSpotter contract. These areas intersect with all six official OPD Police Areas with a focus on areas where gunfire has historically occurred with greater regularity. **Attachment B** to this report is a weekly public ShotSpotter Activation Report for the week; this later report highlights areas of Oakland where ShotSpotter alerts have most recently occurred.

E. A summary of community complaints or concerns about the surveillance technology, and an analysis of the technology's adopted use policy and whether it is adequate in protecting civil rights and civil liberties. The analysis shall also identify the race of each person that was subject to the technology's use. The Privacy Advisory Commission may waive this requirement upon making a determination that the probative value in gathering this information to evaluate the technology's impact on privacy interests is outweighed by the City's administrative burden in collecting or verifying this information and the potential greater invasiveness in capturing such data. If the Privacy Advisory Commission makes such a determination, written findings in support of the determination shall be included in the annual report submitted for City Council review.

Staff reached out to each City Council office to ask about possible community complaints or concerns related to this surveillance technology. No community complaints or concerns were communicated to staff.

OPD is not able to provide the race of each person connected to each activation since shooting suspects are often unknown. Many times, there is data regarding the race of shooting victims or witnesses (may be self-reported); however, this data is not captured in the same system as ShotSpotter and the administrative burden (7,562 total 2022 activations) to constantly connect the two disparate datasets would overwhelm staff capacity. OPD therefore recommends that the PAC makes the determination, that the administrative burden in collecting or verifying this information as well as the associated potential greater invasiveness in capturing such data outweighs the benefit.

F. The results of any internal audits, any information about violations or potential violations of the Surveillance Use Policy, and any actions taken in response unless the release of such information is prohibited by law, including but not limited to confidential personnel file information:

New officers and crime analysts are trained on the ShotSpotter System as part of police officer academies. Officers and analysts are provided with directions that covers login, and how to use different views (e.g., time-period).

OPD officers have automatic access to ShotSpotter notifications when in patrol vehicles equipped with standard vehicle computers via the ShotSpotter Respond System. ShotSpotter creates a log for every sign-in to their system, which includes the level of access the user has (admin view or dispatch view, which is notification only). OPD and ShotSpotter have verified that for 2022, all users who logged into the system were authorized users.

Patrol Officers in vehicles and/or on mobile phones utilize the ShotSpotter Respond System. The Respond System pushes notifications to users – there is no interactivity functionality. ShotSpotter can only audit logins for both the Respond and the Insight program. ShotSpotter and OPD staff have verified that all logins were associated with appropriate active employees. Staff regularly remove access from employee emails where staff separate from City employment.

G. Information about any data breaches or other unauthorized access to the data collected by the surveillance technology, including information about the scope of the breach and the actions taken in response.

There were no identifiable data breaches or unauthorized access during the year of 2022.

H. Information, including crime statistics, that helps the community assess whether the surveillance technology has been effective at achieving its identified purposes.

Table 1: ShotSpotter Activations Resulting in Incident Report for Firearm Crimes by Category in 2022

Cases by Firearm-Related Crime Type	
Homicide	28
Assault with a Firearm	171
Shoot at an Occupied Home/Vehicle	71
Shoot at an Unoccupied Home/Vehicle	91
Negligent Discharge of a Firearm	1,363
Weapons Violations (including exhibit/draw)	11
Carjacking with a Firearm (including attempts)	4
Robbery with a Firearm (including attempts)	19
Total Cases	**1,758**

Table 2: Firearm Recoveries in 2022 Connected to ShotSpotter Activations illustrate Guns Recovered

Guns Recovered by Crime Type	
Homicide	12
Assault with a Firearm	19
Shoot at an Occupied Home/Vehicle	2
Shoot at an Unoccupied Home/Vehicle	0
Negligent Discharge of a Firearm	38
Weapons Violations (including exhibit/draw)	9
Carjacking with a Firearm (including attempts)	1
Robbery with a Firearm (including attempts)	1
Other	1
Total Cases	**83**

- 83 weapons seized.
  - Note: more than one firearm may be from the same incident.
- 967 alerts when advanced situational awareness was provided to responding patrol officers on their way to crime scenes in high danger situations that required specific approach tactics such as multiple shooters**,** high capacity or automatic weapons being used, and drive-by shootings. Some of the alerts had more than one situational awareness tag amounting to 1,230 tags within those 967 alerts.

Table 4: Cases Where ShotSpotter Notifications Resulted in Firearm-Related Crimes being written

Cases by Firearm-Related Crime Type	
Homicide	28
Assault with a Firearm	171
Shoot at an Occupied Home/Vehicle	71

Shoot at an Unoccupied Home/Vehicle	91
Negligent Discharge of a Firearm	1,363
Weapons Violations (including exhibit/draw)	11
Carjacking with a Firearm (including attempts)	4
Robbery with a Firearm (including attempts)	19
Total Cases	**1,758**

I. Statistics and information about public records act requests regarding the relevant subject surveillance technology, including response rates:

There were 25 total PRR in 2022. 20 are closed and *4 remain open.

22-1338
22-2190
22-3599
22-3757
22-4463
22-5180
22-5665
22-6018
22-6019
22-6625
22-6900
22-6911
22-7134
*22-7709
*22-8250
22-8789
22-8850
22-9599
22-9600
*22-9601
*22-9602
22-9774
22-9775
22-9776
22-9777

J. Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year:

Total paid in 2022 was $798,486 for 18.17 square miles of coverage. These fees encompass all services ShotSpotter currently provides to Oakland. There are no additional

charges for meetings, reports, analysis and training. These funds come from OPD's General Purpose Fund.

K. Any requested modifications to the Surveillance Use Policy and a detailed basis for the request:

No requests for policy changes at this time.

OPD is committed to providing the best services to our community while being transparent and instilling procedural justice through daily police activity. This report is compliance with these OPD commitments. OPD hopes that this report helps to strengthen our trust within the Oakland community.

For any questions with this report, please contact Trevelyon Jones, Captain, OPD, Ceasefire Section, at tjones@oaklandca.gov

Respectfully submitted,

Trevelyon Jones

_____

Trevelyon Jones, Captain, OPD, Ceasefire Section

Reviewed by,
Drennon Lindsey,
Deputy Chief, Bureau of Investigations

Steve Valle, Lieutenant
OPD, Criminal Investigations Division

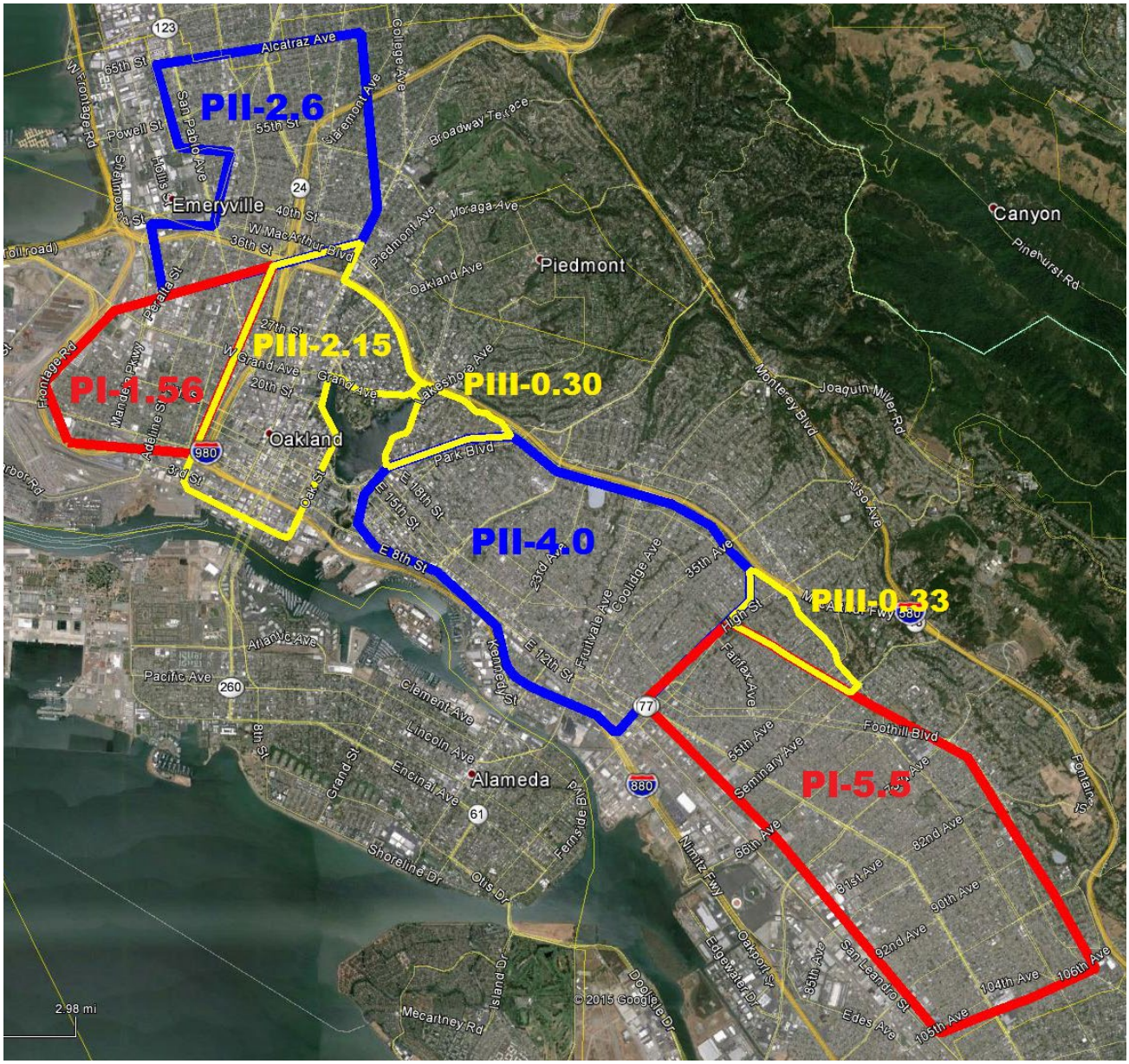
Prepared by:
Tracey Jones, Police Services Manager
OPD, Bureau of Services

Attachment A - Shot Spotter Coverage Areas

Phase I with red borders (Activated in 2006): 6.~~2~~ 0 square miles*
East Oakland: East of High Street to 106th Avenue
West Oakland: East of Highway 980 to Frontage Road

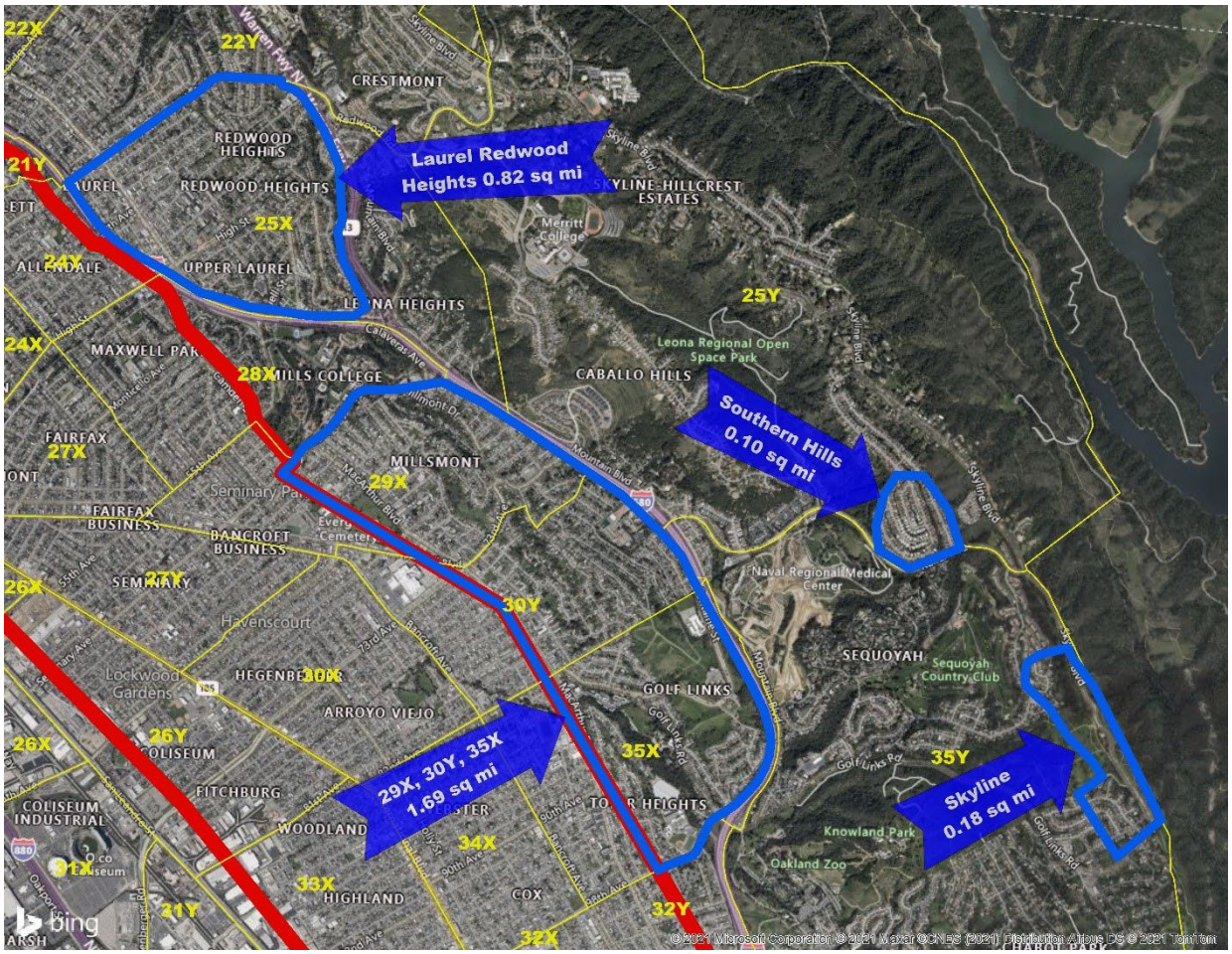
Phase II with blue borders (Activated in 2013): 6.64~~~~ square miles
East Oakland: West of High Street to Park Boulevard
North Oakland: North of Highway 580 to Alcatraz Avenue

Phase III with yellow borders (Activated in 2016): 2.78 square miles
Downtown Oakland: Jack London Square to about West MacArthur Boulevard
Cleveland Height area: East of Lake Merritt to Highway 580 & Park Boulevard
Maxwell Park: East of High Street to Highway 580 & Mills College



* While the original contracted coverage total for Phase I was 6.0 mi², an additional 1.06 mi² of ShotSpotter coverage was added, at no charge, for a total of 7.06 mi² when Phase I service was upgraded and converted to the newer subscription platform in 2011.

Phase IV with blue borders (Activated in 2021): 2.79 square miles
Laurel Redwood Heights: Covering a portion of Beat 25X
Southern Hills: Covering a portion of Beat 25Y
Millsmont / Golf Links: Covering Beats 29X, 30Y, and 35X
Skyline: Covering a portion of Beat 35Y

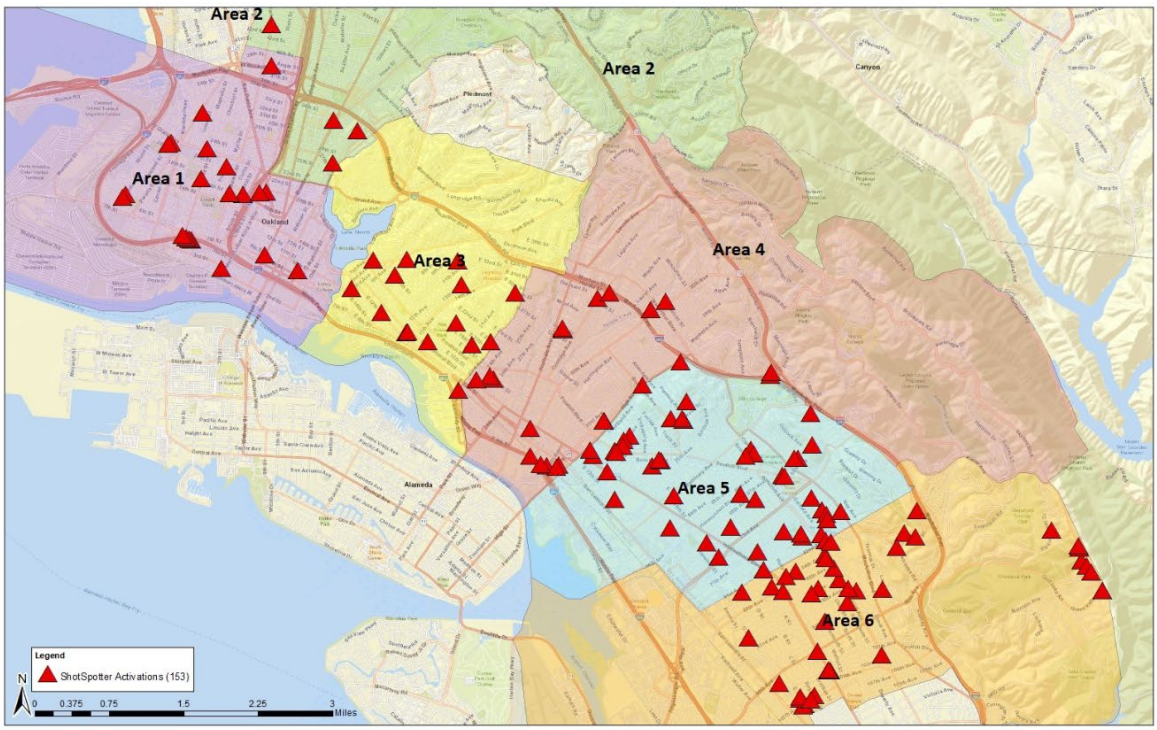

Laurel Redwood Heights 0.82 sq mi
Southern Hills 0.10 sq mi
29X, 30Y, 35X 1.69 sq mi
Skyline 0.18 sq mi
CRESTMONT
REDWOOD HEIGHTS
SKYLINE-HILLCREST ESTATES
Merritt College
Leona Regional Open Space Park
CABALLO HILLS
MILLSMONT
FAIRFAX BUSINESS
BANCROFT BUSINESS
Naval Regional Medical Center
SEQUOYAH
Sequoyah Country Club
GOLF LINKS
Havenscourt
Lockwood Gardens
ARROYO VIEJO
COLISEUM
FITCHBURG
COLISEUM INDUSTRIAL
WOODLAND
HIGHLAND
COX
Knowland Park
Oakland Zoo
22X
22Y
21Y
25X
24Y
24X
28X
27X
29X
27Y
26X
30Y
30X
26Y
35X
35Y
34X
38X
31X
31Y
32Y
32X
bing

ATTACHMENT B

OAKLAND POLICE DEPARTMENT
455 7TH ST., OAKLAND, CA 94607 | OPDCRIMEANALYSIS@OAKLANDNET.COM
CRIME ANALYSIS

Weekly ShotSpotter Activations Report — Citywide
10 Apr. – 16 Apr., 2023

ShotSpotter Activations	Weekly Total	YTD 2021	YTD 2022	YTD 2023	YTD % Change 2022 vs. 2023	3-Year YTD Average	YTD 2023 vs. 3-Year YTD Average
Citywide	153	2,817	2,583	2,269	-12%	2,556	-11%
Area 1	20	275	270	210	-22%	252	-17%
Area 2	7	80	87	74	-15%	80	-8%
Area 3	15	287	260	250	-4%	266	-6%
Area 4	21	435	460	378	-18%	424	-11%
Area 5	46	943	754	607	-19%	768	-21%
Area 6	44	797	752	750	0%	766	-2%



All data sourced via ShotSpotter Insight.

Produced by the Oakland Police Dept. Crime Analysis Unit.

Oakland Police Department

Surveillance Impact Report:
Aircraft Mounted Camera (AMC)/Downlink

1. Information describing the Aircraft Mounted Camera/downlink technology and how it works.

Wescam MX-15

The WESCAM MX-15 does not contain any software, technology, or programs that use Artificial Intelligence, Facial Recognition, gait analysis, or Automated License Plate Reader (ALPR) technology.

The WESCAM MX-15 is an advanced, industry-leading stabilized multi-sensor, multi-spectral imaging system that is renowned for high performance, operator ease-of-use, and reliability. It is ideal for a wide range of objectives, including, Emergency Services, airborne law enforcement, and search and rescue. The system provides cameras for optimal performance in a wide range of conditions such as bright sunlight, overcast/dusk, smoke, and complete darkness. The platform is supported by a suite of advanced image processing algorithms for noise reduction, sharpening, and local area contrast enhancement that aid in object recognition (Object recognition is the ability to detect people, vehicles or objects in relation to their surroundings (i.e., how well you can see something). Superior stabilization is the key to achieving the maximum object detection, recognition, and identification range performance from the cameras.

The WESCAM MX-15 camera comes equipped with technology that allows for easy image tracking and stabilization, regardless of what the aircraft is doing, this allows the officer to focus on what is happening on the other side of the camera, instead of worrying about how to effectively use the camera.

VISLINK DOWNLINK

The Vislink Downlink System will provide the Oakland Police Department with a state-of-the-art airborne video downlink transmit & receive solution that will provide real-time, high quality high-definition airborne images from the aircraft, operating simultaneously, to both fixed and mobile ground receive locations.

This high-quality encrypted/secure video downlink solution will provide real-time actionable video images to both command staff and remote users, allowing for critical decision making, enhancement of officer safety and better allocation of resources.

2. Proposed Purpose

At the direction of the Oakland City Council, Oakland Public Safety Committee, Reimagining Public Safety Task Force and the Oakland Police Department, the Air Support Unit has explored numerous alternatives to the current methods and equipment utilized by the Air Unit. After careful consideration to include, product testing/evaluation, fiscal analysis, stakeholder input, and industry standards, the Department has requested that a fixed wing aircraft be purchased for use by the Air Support Unit. The proposed camera technology which will be installed on the aircraft will allow the Flight Observer (FO) to observe in real time what is occurring on the ground prior to ground units arriving on scene. The fixed wing aircraft which will fly at a much higher altitude than the current aircraft, (3000+ ft above ground level (AGL) vs. 500-700 ft. AGL that the helicopters fly at). This will immediately reduce noise/light pollution as well as the emotional trauma incurred by the citizens of Oakland who have a negative association with the OPD helicopters. A byproduct of this higher altitude is that FO's can no longer look out the window to observe what is occurring below and must rely on a high-definition camera to make their observations. This Camera and any subsequently purchased aircraft mounted cameras will need to be utilized throughout the entirety of the flight while responding to dispatched calls as well as to proactively be on the lookout for criminal activity much as an officer would look out their vehicle window while on routine patrol. Aircraft mounted cameras have existed on the OPD helicopters for over two decades. This technology however is outdated and ineffective to perform the tasks that the Air Support Unit is currently tasked with.

The downlink component of the system allows the video and pictures captured by the AMC to be streamed via a secure wireless connection to those devices authorized and approved by the department. Utilizing downlink will provide Commanders, Officers, City Leaders and other Emergency Responders a greater overall picture of what is occurring. Downlink can be utilized during natural disasters (earthquakes, fires, flooding etc.) to allow Emergency personnel to assess evacuation routes, direct responders, and coordinate emergency efforts. The downlink can also be used to ensure the efficiency and accountability of officers on the ground. Additional uses of the downlink include utilization during protests to reduce the need of officers being in direct contact with suspects concealing themselves within the crowd, report on direction of travel, and create greater standoff distance with those peacefully protesting. Downlink may also improve situational awareness of unlawful sideshows. This increased situational awareness can be used to assist in de-escalation efforts of various critical instances.

3. Location:

OPD aircraft and their associated technologies to include the WESCAM MX-15 and VISLINK downlink system may be deployed within the city of Oakland in accordance with the Air Support Unit Deployment Plan as directed by the Chief of Police or their designees. The OPD helicopters and airplane serve as a patrol unit in the sky and may respond anywhere within the jurisdiction of the Oakland Police Department. The OPD Air Support Unit is occasionally requested to assist with investigations in neighboring jurisdictions and would respond as available to assist with those in

accordance with mutual-aid policies and MOU's currently in place. All policies for the use of the associated equipment would be in effect as stated in the Aircraft Mounted Camera Use Policy.

4. Impact:

As this is an initial SIR and the use policy is currently under review, there are no prior records or documentation regarding previous deployments and its effects both positive or negative.

5. Mitigations:

As with Body Worn Camera (BWC) video currently obtained by the department, all video recorded by the AMC is subject to disclosure under a Public Records Act (PRA) request. Video is also subject to audit by Internal Affairs, the Community Police Review Agency (CPRA) and command staff. Random audits may be conducted by the department at their discretion to ensure that members are in compliance with the AMC use policy (DGO I-29). The ASU Supervisor will also be responsible for ensuring that each member authorized to operate the AMC and downlink equipment has been properly trained in the authorized and prohibited uses of such equipment. Training shall be documented with the appropriate records and forms as designated by the department.

6. Data Types and Sources:

The AMC will record using industry standard file types: JPEG, mov, mp4, wav, or RAW. Such files may contain standard color photograph, standard color video, or other imaging technology, such as thermal. The AMC does not record or transmit audio in any way.

7. Data Security:

All AMC data storage devices (SD Card, Flash Drive, Portable Hard Drive) will be secured in a manner (e.g. lockbox) only accessible to Air Support Unit (ASU) personnel. All evidence from ASU data devices shall be uploaded to the EVIDENCE.COM server and then immediately removed from the drive. See Attachment 4 for OPD Data Retention Policy Time Frames

8. Fiscal Cost:

The Wescam MX-15 camera and the Vislink Downlink equipment was included in a RFQ for the aircraft and mission equipment. See Oakland City RFQ 271104.

MX-15- $724,881.00

Vislink Downlink system – $265,000.00

Third Party Dependence:

All data collected by the technology to include video recording will be stored in the EVIDENCE.COM server (currently utilized for all BWC data storage). This is not anticipated to increase the cost or decrease the effectiveness of the city's current data storage capabilities.

9. Alternatives:

The Aircraft Mounted Camera SUP (***Attachment A),*** Section 1, "Alternatives Considered", explains that "OPD could continue the status quo of utilizing the OPD Helicopter with the FLIR 8500 Series camera as well as gyro stabilized binoculars to monitor activities occurring on the ground. Continuing in this manner will require the air asset to fly at an altitude considerably lower causing increased sound/light pollution and trauma associated with the helicopter to the citizens of Oakland.

The Alternatives section also considers drone usage. While drones play an integral part in the protection of Oakland residents and visitors, they are limited in their capabilities. The current flight time for drones is approximately 25-30 minutes and speeds of 25 mph Drones are limited to line of sight and cannot operate in an area greater than 2-3 blocks. Drones are currently not capable of assisting during vehicle pursuits that exceed these speeds or distances as stated above. Due to the busy airspace surrounding the Oakland International Airport UAV's are extremely limited to the locations altitudes and ranges that they can fly. UAV's are also limited in their deployment availability. Drones require approval prior to each deployment. Once approval is obtained the operator must acquire the equipment, respond to the scene, wait for approval from the FAA and then launch the drone. By this time an incident has likely evolved greatly and may have already concluded prior to the utilization of the drone. OPD aircraft typically fly for 1-2 hours and with the purchase of a fixed wing aircraft will have greater flight capabilities with response times frequently of under 1 minute from dispatch to scene arrival.

OPD does have access to outside agency air assets equipped with cameras such as CHP and ACSO. However, OPD must request those agencies to respond for each incident. This creates a significant delay in response times as each of those agencies are located outside of the city of Oakland (CHP operates from the Napa County Airport 30 NM away and ACSO 19 NM). This process can take a significant amount of time which could negatively impact the outcome of a critical incident. Additionally, these neighboring agencies are responsible for large areas of land outside of Oakland (CHP Golden Gate Division covers nearly 7,000 sq miles and ACSO 739 sq. miles). Due to the unique weather patterns experienced by the City of Oakland weather frequently prohibits neighboring agencies response to the city of Oakland for assistance. OPD can better respond to dangerous situations by equipping our own aircraft with cameras capable of the same level of service provided by neighboring agency aircraft and responding in a timely manner.

10. Track Record:

During previous critical incidents the Oakland Police Department has relied on outside agencies to include the California Highway Patrol, Alameda County Sheriff's Office, and Contra Costa Sheriff's office to provide recordings of critical incidents that have involved officers of the Oakland Police Department.

During the George Floyd Demonstrations in 2020 CHP was again requested to provide assistance to the City of Oakland. CHP in addition to the Oakland Air Support Unit provided updates to command and city leaders on the ground. CHP however was able to provide real time video from overhead to the Emergency Operations Center with City officials such as the Mayor, City Administrator, Police, Fire and Emergency Services Personnel. This Downlink technology was specifically requested by city leaders for events such as this and has been used successfully on many occasions.

In 2020 Contra Costa Sheriff's office captured an Officer involved shooting involving Richmond and Oakland Police Officers. CCCSO was overhead and recording when an armed murder suspect intentionally rammed several Oakland police vehicles in the city of Richmond. The entire shooting was captured by the Sheriff's helicopter and the video was used by the respective investigative bodies after the incident.

In November 2021 Oakland Officers were fired upon by a carjacking suspect. The vehicle was tracked for an extended time by ground and air resources. While attempting to detain the subject CHP air was overhead recording with their aircraft mounted camera. Video showed the subject ramming multiple patrol cars and later engaging several officers. This incident led to an officer involved shooting that was captured by both BWC and the aircrafts camera. This video was critical to the subsequent investigations by the Criminal Investigations Division, Internal Affairs as well as the Community Police Review Agency.

11. Privacy Considerations

AMC Operators shall not intentionally record or transmit images of any location where a person would have a reasonable expectation of privacy (e.g. residence, enclosed yard, enclosure) unless actively searching for a victim, suspect, or evidence related to a crime etc. When OPD Aircraft are being flown and the AMC is being utilized, operators will take steps to ensure the camera is focused on the areas necessary to the task and to minimize the inadvertent collection of data about uninvolved persons or places. Operators and observers shall take reasonable precautions, such as turning imaging devices away, to avoid inadvertently recording or transmitting images of areas where there is a reasonable expectation of privacy.

Attachments

1 AMC/Downlink Surveillance Use Policy
2 Wescam Documents/manual
3 Downlink Documents/manual