City and County of San Francisco
Municipal Transportation Agency
One South Van Ness Ave. 7th floor
San Francisco, California 94103

Second Amendment to Agreement for Operation and Management of Off-Street Parking Facilities, Group B, Contract No. SFMTA-2011/12-10

THIS AMENDMENT (this "Amendment") is made and is effective as of January 31, 2018, in San Francisco, California, by and between **IMCO Parking, LLC** ("Manager" or "Contractor"), and the San Francisco Municipal Transportation Agency, hereinafter referred to as "SFMTA" or "City."

RECITALS

A. City and Manager have entered into the Agreement (as defined below).

NOW, THEREFORE, Manager and the City agree as follows:

1. **Definitions.** The following definitions shall apply to this Amendment:

1a. Agreement. The term "Agreement" shall mean the Agreement dated December 12, 2011, as modified by the First Amendment, dated June 16, 2017, and by this Second Amendment, dated January 31, 2018.

1b. Contract Monitoring Division. Effective July 28, 2012, with the exception of Sections 14B.9(D) and 14B.17(F), all of the duties and functions of the Human Rights Commission under Chapter 14B of the Administrative Code (LBE Ordinance) were transferred to the City Administrator, Contract Monitoring Division ("CMD"). Wherever "Human Rights Commission" or "HRC" appears in the Agreement in reference to Chapter 14B of the Administrative Code or its implementing Rules and Regulations, it shall be construed to mean "Contract Monitoring Division" or "CMD" respectively.

1c. Other Terms. Terms used and not defined in this Amendment shall have the meanings assigned to such terms in the Agreement.

2. Modifications to the Agreement.

2a. Extension of Term. The term of the Agreement is hereby extended by 18 months, pursuant to the terms outlined in Section 5.1 of the Agreement. The revised expiration date of the Agreement is July 31, 2019.

2b. PCI Data Security Standards. Section 18.42 is added to the Agreement as follows:

18.42 PCI Data Security Standards

18.42.1 Manager shall manage credit card payment transactions for the Facility in accordance with Payment Card Industry Data Security Standards ("PCI DSS") as established by the PCI Security Standards Council ("PCI SCC"), which may be found at https://www.pcisecuritystandards.org, and as the PCI Council may update those requirements and publish them at that website. Capitalized terms in this Agreement pertaining to PCI DSS, if not defined in this Agreement, shall have the meanings provided by PCI SCC, and "PCI compliance" as used herein shall mean compliance with PCI DSS.

18.42.2 Manager shall operate the Facilities using Parking Access and Revenue Control System (PARCS) equipment provided by the City. The PARCS vendor, pursuant to its contract with the City, is responsible for establishing and maintaining the PCI compliance of the PARCS equipment and software configuration and deployment at the Facility (As described in Appendix A to this Amendment.). The PARCS vendor's responsibilities are described in Appendix A of this Agreement. Manager is not liable for the negligence of the PARCS vendor or failure of the PARCS vendor to ensure that the PARCS is PCI compliant or for the PARCS vendor's failure to otherwise comply with its obligations in Appendix A.

18.42.3 The City and the PARCS vendor will collaborate to design, install and implement an IT network controlled by the City by which the PARCS equipment at the Facilities will communicate with the City, the PARCS vendor, the Manager, and any other entities approved by the City. Manager will collaborate with the City and the PARCS vendor to install and implement a firewall that will connect to the Payment Express card readers in the PARCS payment stations for processing of credit card transactions. When the City's IT network and the Manager's firewall and network are both deployed, Manager and City shall not make any changes to their respective networks without first notifying the other party, in writing.

18.42.4 In its use of the PARCS equipment and software to operate the Facilities, Manager shall utilize business procedures and practices and data security procedures and practices that comply with the most current PCI DSS.

18.42.5 Manager shall not store, retain or otherwise utilize Credit Card Data except as required by PCI DSS and only to the extent necessary to identify a transaction for accounting and refund purposes.

18.42.6 When the Manager services any part of the PARCS pay stations, it shall visually inspect the pay stations to discover sniffers and other unauthorized equipment installed in the pay stations, and shall notify the City of any such unauthorized equipment or other anomalies it discovers.

3. Effective Date. Each of the modifications set forth in Section 2 shall be effective on and after the date of this Amendment, as stated above.

4. Legal Effect. Except as expressly modified by this Amendment, all of the terms and conditions of the Agreement shall remain unchanged and in full force and effect.

The remainder of this page has been intentionally left blank.

IN WITNESS WHEREOF, Contractor and City have executed this Amendment as of the date first referenced above.

San Francisco
Municipal Transportation Agency

APPROVED:

By: ______________________

Edward D. Reiskin
Director of Transportation

Approved as to Form:

Dennis J. Herrera
City Attorney

By: ______________________
Robert K. Stone
Deputy City Attorney

MANAGER: IMCO Parking LLC

APPROVED:

By: ______________________
Ed Danyluk
Regional Manager, Western U.S.

APPENDIX A

Below, for reference, is detail regarding the PARCS Vendor's contractual responsibilities regarding PCI Data Security. The text is excerpted from the conformed agreement #SFMTA-2015-36, dated December 1, 2016, between the City and Skidata, Inc.

63. PCI Data Security Requirements.

a. The requirements referenced in this Section are established by the PCI Security Standards Council ("PCI SCC") and may be found at https://www.pcisecuritystandards.org , and as the PCI Council may update its requirements and publish them at that website.

b. Capitalized terms in this Section, if not defined in this PARCS Agreement, shall have the meanings provided by PCI SCC. For the term of this PARCS Agreement and any related maintenance or other service agreement between the SFMTA and the City concerning the PARCS, the PARCS Application shall be validated by a Payment Application Qualified Security Assessor (PA-QSA). A Vendor whose application has achieved PA-DSS certification must then be listed on the PCI Council's list of PA-DSS approved and validated payment applications.

c. Vendor shall ensure that the PARCS Software meets all applicable requirements of the PCI SCC's Data Security Standards. Vendor shall provide a letter from its Qualified Security Assessor (QSA) affirming its compliance with PCI DSS requirements and current PCI compliance certificate or proof thereof. Vendor shall provide to the SFMTA proof of PCI compliance for each version of PARCS software that is installed during the term of this PARCS Agreement, including the Warranty Period and any Maintenance Period. Vendor shall be responsible for furnishing City with proof of PCI compliance from a QSA 30 days prior to the expiration of said certificates. In addition, the City may at any time, at its own cost and following reasonable notice, audit Vendor's compliance with the PCI DSS and other data security requirements stated in the PARCS Agreement, and Vendor shall fully cooperate with such audit. All applicable updates to the Licensed Software shall be PCI DSS certified.

d. Vendor represents that the PARCS retains credit card data in a manner that complies with PCI DSS requirements, and does so only to the extent necessary to identify a transaction for accounting and refund purposes. Vendor represents that the credit card readers in payment stations and imbedded software operating such readers for the PARCS will be supplied by the Gateway provider recommended by Vendor and approved by the SFMTA. The data connection between said card readers and software and the PARCS shall not allow Primary Account Number (PAN), credit card number, Credit Card Verification Code (CCV), Credit Card Expiry date or cardholder name to be accessed by the PARCS or a PARCS operator. Vendor shall maintain said credit card readers. The payment processor shall be responsible for electronically monitoring the credit card readers for malfunctions, sniffers, and data security. When Vendor services pay stations, Vendor shall visually inspect the pay stations to discover sniffers and other unauthorized equipment.

Gateway providers shall have appropriate Payment Card Industry Data Security Standards (PCI DSS) certification as service providers, as determined by PCI SCC. (See https://www.pcisecuritystandards.org/index.shtml). PARCS Components that process or retain data from PIN Debit Cards shall be validated against the PCI SCC's PIN Transaction Security (PTS) program.