TCRP LEGAL RESEARCH DIGEST 48: LEGAL ISSUES CONCERNING TRANSIT AGENCY USE OF ELECTRONIC CUSTOMER DATA

Appendix A—List of Transit Agencies Responding to the Survey

Appendix B—Survey Questions

Appendix C—Summary of the Transit Agencies' Responses to the Survey

Appendix D—Documents Provided by Transit Agencies Responding to the Survey

APPENDIX A—LIST OF TRANSIT AGENCIES RESPONDING TO THE SURVEY

1. Ann Arbor Transportation Authority, Ann Arbor, MI
2. Antelope Valley Transit Authority, Lancaster, CA
3. Belle Urban System, The, Racine, WI
4. Berkshire Regional Transit Authority, Pittsfield, MA
5. Capital Area Transportation Authority, Lansing, MI
6. Capital District Transportation Authority, Albany, NY
7. Central Florida Regional Transportation Authority d/b/a Lynx, Orlando, FL
8. Central Ohio Transit Authority, Columbus, OH
9. Centre Area Transportation Authority, State College, PA
10. City of Cheyenne Transit Program, Cheyenne, WY
11. City of Alexandre, LA
12. City of Glendale Transit, Glendale, AZ
13. City of Madison Metro Transit, Madison, WI
14. City of Raleigh, GoRaleigh, Raleigh, NC
15. City of Visalia, Transit Division, Visalia, CA
16. City Utilities of Springfield, Springfield, MO
17. Cobb Community Transit, Marietta, GA
18. Connecticut Department of Transportation, Newington, CT
19. Corpus Christi Regional Transportation Authority, Corpus Christi, TX
20. CT Transit, Hartford, CT
21. Durham Area Transit Authority, GoDurham, Durham, NC
22. Fresno Area Express, Fresno, CA

23. Golden Empire Transit District, Bakersfield, CA
24. Greater Attleboro Taunton Regional, Taunton, MA
25. Greater Cleveland Regional Transit Authority, Cleveland, OH
26. Greater Hartford Transit District, Hartford, CT
27. Greater Lynchburg Transit Company, Lynchburg, VA
28. Greater Lafayette Public Transportation, Lafayette, IN
29. La Crosse Municipal Transit, La Crosse, WI
30. Lake Charles Transit System, Lake Charles, LA
31. Laketran, Painesville Township, OH
32. Lane Transit District, Eugene, OR
33. Manchester Transit Authority, Manchester, NH
34. METRA, Chicago, IL
35. Metro Regional Transit Authority, Akron, OH
36. Metropolitan Transportation Authority, New York, NY
37. Metropolitan Transportation Commission, Oakland, CA
38. Milford Transit District, Milford, CT
39. Milwaukee County Transit System, Milwaukee, WI
40. Montgomery Area Transit System, The M, Montgomery, AL
41. Municipality of Anchorage, Public Transportation Department, Anchorage, AK
42. Muskegon Area Transit System, Muskegon Heights, MI
43. Niagara Frontier Transportation Authority, Buffalo, NY
44. Ohio Valley RTA, Wheeling, WV
45. Omnitrans, San Bernardino, CA
46. ORCA Regional Coordination Program, Seattle, WA

47. Port Authority of Allegheny County, Pittsburgh, PA

48. Pueblo Transit, Pueblo, CO

49. Regional Transportation District, Denver, CO

50. Salem-Keizer Transit, Salem, OR

51. Sarasota County Area Transit, Sarasota, FL

52. Sioux Area Metro, Sioux Falls, SD

53. Space Coast Area Transit, Cocoa, FL

54. Sunline Transit Agency, Thousand Palms, CA

55. Topeka Metropolitan Transit Authority, Topeka, KS

56. TriMet, Portland, OR

57. Valley Regional Transit, Meridian, ID

58. Valley Transit District, Derby, CT

59. Votran, South Daytona, FL

60. Westchester County Department of Public Works and Transportation, Mount Vernon, NY

61. Western Reserve Transit Authority, Youngstown, OH

62. VIA Metropolitan Transit, San Antonio, TX

APPENDIX B—SURVEY QUESTIONS

TRB TRANSPORTATION RESEARCH BOARD OF THE NATIONAL ACADEMIES

SURVEY QUESTIONS

If you prefer an electronic copy of the survey please contact the Thomas Law Firm by email at:
lwthomas@cox.net

TCRP J-5, STUDY TOPIC 16-02, LEGAL ISSUES CONCERNING TRANSIT AGENCY USE OF ELECTRONIC CUSTOMER DATA

Agency Name: _____

Name of Employee: _____

Job Title: _____

Contact telephone/ cell phone number: _____ _____

Email address: _____

Educational Background: _____

Legal Training: YES NO (If "yes" describe) _____

How many years have you been with the agency? _____

****

NOTE

The term "electronic customer data" used herein refers to data collected by transit agencies by contactless (or other) electronic payment systems that accept payment by a smart card, a customer's credit or debit card, and/or mobile device. The term electronic customer data includes personally identifiable information, financial data, travel data (*e.g.*, time of travel and points of origin and destination), and real-time location data.

1. Is your agency using one or more contactless (or other) electronic payment system(s) for customers to pay for transit?

(please circle) YES NO

IF YOUR ANSWER IS "YES," PLEASE RESPOND TO THE FOLLOWING QUESTIONS AND REQUESTS.

(If insufficient space is allotted for your responses below, please feel free to place your responses on additional sheets of paper and attach them to the survey.)

2. Please identify the type of contactless (or other) electronic payment system or systems that your agency is using presently.

_____

_____

3. Is your agency collecting customers' personal data as defined in the above Note with its present electronic payment system?

(please circle) YES NO

If your answer is "Yes," please describe the types of personal data that your agency is collecting.

_____

_____

4. Is your agency planning to adopt a new electronic payment system or systems?

(please circle) YES NO

If your answer is "Yes," please describe:

(a) the system being adopted or that is under consideration for adoption; and

_____

_____

(b) the types of data that your agency will be collecting with the new system.

_____

_____

5. With your current or proposed electronic payment system are customers able:

(a) To use their credit and debit cards to pay for transit?

(please circle) YES NO

If your answer is "Yes" to question 5(a), please provide details.

_____

_____

(b) To use Near Field Communications (NFC)-enabled mobile phones or other mobile devices to pay for transit?

(please circle) YES NO

If your answer is "Yes" to question 5(b), please provide details.

_____

_____

6. If your agency is using customers' personal data, please describe how the data is being used:

a) For the benefit of the agency:

_____

_____

b) For the benefit of customers:

_____

_____

7. (a) Does your agency have an agreement, terms of use, and/or privacy policy that it uses in connection with its electronic payment system?

(please circle) YES NO

If your answer is "Yes" to question 7(a), please provide a copy of or a link to any agreement(s), terms of use, and/or privacy policy that your agency uses.

_____

_____

(b) Does your agency have a website that collects customers' personal data when they use the website?

(please circle) YES NO

If your answer is "Yes" to question 7(b), please provide a copy of or a link to any agreement, terms of use, and/or privacy policy that your agency uses for the website.

_____

_____

8. (a) If not answered by the agreements, terms of use, and privacy policy or policies provided in response to question 7(a) and/or 7(b), please state:

(1) Who owns the personal data collected by your agency?

_____

_____

(2) Who has access to the personal data?

_____

_____

(3) What personal data may be accessed and under what circumstances?

_____

_____

(4) How long may data be retained, stored, or archived?

_____

_____

(5) What safeguards are used to prevent hacking and misuse of customers' personal data?

_____

_____

9. (a) Does your agency have an agreement with a contractor or agent (or other holder of customers' personal data) for the purpose of collecting, using, disclosing, and/or retaining data obtained by a contactless (or other) electronic payment system?

(please circle) YES NO

If your answer is "Yes," please provide a copy of or a link to any such agreement or agreements.

_____

_____

(b) If not answered by your response to question 9(a), how does your agency describe or define the obligations of your agency, its contractor(s), or other holders of customers' personal data?

_____

_____

10. Is your agency "monetizing" customers' personal data that the agency (or a contractor or agent on behalf of the agency) collects?

(please circle) YES NO

If your answer is "Yes," please describe the ways in which the agency is monetizing customers' personal data.

_____

_____

11. Does your agency have any agreements with third-party developers that involve the sharing of customers' personal data for the purpose of offering customers certain benefits or options?

(please circle) YES NO

If your answer is "Yes," please provide details and/or a copy of or a link to any such agreement(s).

_____

_____

12. Are there any federal or state constitutional provisions, laws, regulations, or policies of which you are aware that apply to your agency's (or contractor's) collection, use, disclosure, or retention of customers' personal data?

(please circle) YES NO

_____

_____

If your answer is "Yes," please identify and provide a copy of or a link to any such agreement or agreements.

_____

_____

13. If your agency accepts payment for transit fares by credit or debit cards has your agency (or a contractor or agent on behalf of your agency) taken steps to comply with the Payment Card Industry Data Security Standards (PCI DSS)?

(please circle) YES NO

If your answer is "Yes," please provide details and/or a link to or a copy of any agreement(s) between your agency and any financial institution and/or any credit or debit card company regarding PCI DSS-compliance.

_____

_____

14. Within the past five years have there been any legal actions brought against your agency (or a contractor or agent of your agency):

(a) alleging a violation of a customer's right to privacy?

(please circle) YES NO

If your answer is "Yes," please provide details and a citation to any case(s) or decision(s).

_____

_____

(b) alleging that a customer's data was compromised because of a breach of security of their personal data?

(please circle) YES NO

If your answer is "Yes," please provide details and a citation to any case(s) or decision(s).

_____

_____

15. If your answer is "Yes" to question 14(a) and/or 14(b), please state the basis of the claim(s) (*e.g.*, breach of contract, negligence, violation of a federal or state constitutional right to privacy, violation of a federal or state privacy and/or data-breach statute, and/or violation of a right to privacy at common law).

_____

_____

16. In regard to questions 14 and 15, does your agency have sovereign immunity for any such claim or claims?

(please circle) YES NO

If your answer is "YES," please provide details.

_____

_____

****

Please return your completed survey to:

The Thomas Law Firm
ATTN: Larry W. Thomas, J.D. Ph.D.
2001 L Street, N.W., Suite 500
Washington, D.C. 20036
Tel. (202) 495-3442

E-mail: lwthomas@cox.net

APPENDIX C—SUMMARY OF THE TRANSIT AGENCIES' RESPONSES TO THE SURVEY

Please note that for the purpose of the survey, the term "electronic customer data" refers to data collected by transit agencies by contactless or other electronic payment systems that accept payment by a smart card, a customer's credit or debit card, and/or a mobile device. The term "customer electronic data" is defined to include personally identifiable information (PII), financial data, travel data (e.g., time of travel and points of origin and destination), and real-time location data.

Questions and Responses

1. Is your agency using one or more contactless (or other) electronic payment system(s) for customers to pay for transit?

(please circle) YES NO

If an agency answered "Yes" to the question, the agencies were asked to respond to the questions and requests numbered 2 through 16.

Of the 62 transit agencies responding to the survey, 29 agencies stated "Yes."[787]

It may be noted that the Metropolitan Transportation Authority or MTA includes New York City Transit Authority (NYCT), Metro-North Commuter Railroad (MNR), Long Island Rail Road (LIRR), MTA Bus Company, and Staten Island Railway (SIR).

The ORCA (One Regional Card for All) is a smart card fare-payment system for the Puget Sound region. The ORCA Regional Fare Coordination Program includes Community Transit, Everett Transit, King County Metro, Kitsap Transit, Pierce Transit, Sound Transit, and Washington State Ferries.

Because some of the six agencies that answered "No" to the question still responded to some of the questions in the survey, the agencies are identified by an asterisk when they answered a survey question.

2. Please identify the type of contactless (or other) electronic payment system or systems that your agency is using presently.

The Capital District Transportation Authority explained in more detail that it

[787] Berkshire Regional Transit Authority, Capital Area Transportation Authority, Capital District Transportation Authority, Central Florida Regional Transportation Authority, City of Visalia, Cobb Community Transit, Connecticut Department of Transportation, Greater Cleveland Regional Transit Authority, Laketran, Lane Transit District, Manchester Transit Authority, Metra, Metro Regional Transit Authority, Metropolitan Transportation Authority, Metropolitan Transportation Commission, Milwaukee County Transit System, Municipality of Anchorage, Public Transportation Department, OmniTrans, ORCA Regional Coordination Program, Port Authority of Allegheny County, Regional Transportation District, Salem-Keizer Transit, Space Coast Area Transit, Sunline Transit Agency, Topeka Metropolitan Transit Authority, TriMet, Valley Regional Transit, Westchester County Department of Public Works and Transportation, and VIA Metropolitan Transit.

> uses a SPX-Genfare provided fare collection system, which includes FastFare™ fareboxes placed on-board all fixed route vehicles capable of processing cash magnetic stripe, contactless limited use Ultalight C cards. DesFire long term smart cards, 2D bar codes, proximity cards, and DesFare adhesive smart media. This electronic payment system includes a fully hosted central data system for ridership and revenue reconciliation, point of sale, and customer account management for internal management staff, while offering customers retail and administrative point of sale terminals, and customer facing web portals to purchase and replenish all forms of CDTA payment media. The current system is also capable of processing EMV compliant payment cards and mobile ticketing transactions in the future.

As for the Metropolitan Transportation Authority, its approach is

> based on the electronic fare collection system serving NYCT subways and buses, MTA bus company's buses, SIR's railway cars and certain other regional transportation providers. MNR and LIRR have implemented pilots of mobile ticketing applications whereby customers can pay for commuter rail rides using a mobile device. All of the same privacy policies apply to those applications as apply to the Metrocard and NFPS systems described below.

Furthermore, the MTA stated:

> The current system is based on the MetroCard, which is a magnetic strip closed-loop card that serves NYCT subways and buses, MTA Bus Company's buses, SIR's railway cars and certain other regional transportation providers. The MetroCard is a 10 mil polyester card that can provide stored value (pay-per-ride) and period pass (7-day or 30-day, unlimited ride) functionality, all of which are pre-funded by the customer at purchase or reload. The Fare Products are activated through magstripe read/write technology at a swipe read/write block or a transport unit, which have been incorporated into various devices across the MetroCard System.

The Metropolitan Transportation Commission explained that the MTC manages a closed-loop contactless payment system for public transit used by 22 regional operators, under the brand name of Clipper®.

The Milwaukee County Transit System has "a card-based contactless smart card system. Fare box devices have smartcard read/write capability using NFC. Fare box devices do not directly accept credit/debit cards for fare payment."

ORCA's current system "is closed loop [that] uses contactless MIFARE DESFire EV1 card. Tap at reader to board or validate trip. Data is up- and downloaded at least daily between back end and card readers. Financial settlement is processed through Vix managed back office."

As for the Port Authority of Allegheny County, its "Automated Fare Collection System (AFCS) uses an RFID Mifare 1K Classic smart card and Limited Use RFID paper tickets. It is a closed payment, card based payment system. The cards are designed using ISO/IEC 14443 standards."

Other agencies responding to the survey also briefly described the contactless or other electronic payment system being used by their agency.[788]

3. Is your agency collecting customers' personal data as defined in the above Note with its present electronic payment system?

(please circle) YES NO

Twenty-two agencies answered "Yes" to the question.[789] Nine agencies answered "No."[790]

If your answer is "Yes," please describe the types of personal data that your agency is collecting.

---

[788] Berkshire Regional Transit Authority ("Charlie Card by Scheidt and Bachman administered by the MBTA); Capital Area Transportation Authority (credit and debit cards); Central Florida Regional Transportation Authority (name, address, and last 4 digits of card pass through portal to Bank of America merchant services); City of Raleigh, GoRaleigh (currently in the process of implementing smart cards); City of Visalia Transit Department (Apriva Pay Plus (mobile payment and swipe), authorize.net (credit card swipe and online payment only); Cobb Community Transit (Breeze card, a Cubic product); Connecticut Department of Transportation (Via, our contracted transit providers, accepting credit card payments via ticket vending machines); CT Transit (implementing smart cards in 2017); Greater Cleveland Regional Transportation Authority (TVMs/CSKs, Web store and customer server POS); Laketran (smart card accepted on bus, credit or debit cards accepted online); Lane Transit District (customer Service counter (POS), on-platform ticket vending machines, LTD Web store); Manchester Transit Authority (online fare media via credit card; smart cards with either electronic pass (daily, monthly, etc.) or stored value card); Metra identified: Verifone MX915 devices utilize contact Point of Sale (POS) transactions; Ticket by Internet (TBI); Mobile Ticketing; and Credit Card Ticket Vending Machines (CCTVM); Metro Regional Transit Authority (METRO primarily using magnetic fare media but just started to switch to smart cards); Municipality of Anchorage, Public Transportation Department (automated ticket machine); Omnitrans (stating that credit and debit cards can be used at ticket vending machines or online store to purchase traditional fare media (bus passes)); Regional Transportation District (contactless: MiFare Cards (a.k.a. Smart Media); other–Aloha/NCR systems (staffed static sales outlets); Gateway Galaxy systems (mobile sales outlets); Scheidt & Bachmann ticket vending machines; Opal ticket vending machines; and vendor-operated Web sites); Salem Area Mass Transit District (agency uses magnetic strip fare cards for day passes, 30-day passes, and multiple-day passes between 1 and 30 days); Space Coast Area Transit (use of credit cards for purchasing transit tickets at bus terminals, over the telephone, and online at agency's Web site); Sunline Transit Agency (pass sales on Web site); Topeka Metropolitan Transit Authority (sells tickets and passes on agency's Web site, at ticket vending machines, payment kiosks, and via "credit card machine"); TriMet (mobile ticketing app, ticket vending machines, and online store that allows "web payments"); Westchester County Department of Public Works & Transportation (MTA Metrocard System); and Via Metropolitan Transit (customer bank-issued credit cards).

[789] Capital Area Transportation Authority, Capital District Transportation Authority, Central Florida Regional Transportation Authority, City of Visalia, Connecticut Department of Transportation, Greater Cleveland Regional Transit Authority, Laketran, Lane Transit District, Metra, Metropolitan Transportation Authority, Metropolitan Transportation Commission, Milwaukee County Transit System, OmniTrans, ORCA Regional Coordination Program, Port Authority of Allegheny County, Regional Transportation District, Salem-Keizer Transit, Space Coast Area Transit, Topeka Metropolitan Transit Authority, TriMet, Valley Regional Transit, and VIA Metropolitan Transit.

[790] Berkshire Regional Transit Authority, Cobb Community Transit, CT Transit,* Greater Lynchburg Transit Company,* Manchester Transit Authority, Metro Regional Transit Authority, Municipality of Anchorage, Public Transportation Department, Niagara Frontier Transportation Authority,* and Sunline Transit Agency.

The Capital Area Transportation Authority explained that CATA collects information on its Web site in two different ways:

> First, we use server logs to collect anonymous, aggregate information (such as browser type, ISP, IP address, referring/exit pages, platform type, date/time stamp, number of clicks) from all visitors to the site. Our site also uses a standard technology called "cookies" to collect information about how the site is used. Information gathered through cookies may include the pages viewed and the amount of time spent on CATA's website. This type of information is typically not linked to any personally identifiable information and is used primarily in the aggregate to generate statistical reports that help us refine and improve the site.
>
> Second, we require certain information when you use various services on the site. For example, when you contact us by email, we may collect your email address and any other personal information you provide. When you subscribe to any of our notification systems you must provide your name and a valid email address. If you purchase items from the online pass sales area, CATA and its payment processing partner will collect additional information necessary for payment and delivery. If you apply for employment or to be included on the bidders registration list through our site, we will collect information such as your name, address and other employment or business-related information.

CATA also stated that it "complies with the requirements of the Children's Online Privacy Protection Act (COPPA) and the FTC's Rule interpreting COPPA (16 CFR SS 512). The site is not directed to children, and we do not knowingly collect any personally identifiable information on the site from children under 13 years of age."

The customers' PII collected by the Capital District Transportation Authority includes travel (real time location) information about their trips. In addition, each registered smart card customer provides his or her name; email address; telephone number; boarding location, time, and date; and purchase location, time, and date. Credit card information is not collected.

The Metropolitan Transportation Authority stated:

> Each MetroCard's transaction history is held centrally in a mainframe computer called the Area Controller. All data tied to MetroCard usage and sales and credit/debit authorization requests are transmitted via a station controller which stores the information locally if communications are not available, in batched transmissions at timed intervals from vending machines, station booth terminal or turnstiles. Several key data components have higher priorities in the MetroCard System and are uploaded as soon as they arrive. These include authorization requests associated with credit/debit sales at vending machines and the backend portion of the MetroCard System that tracks credit/debit confirmations. Device maintenance messages are also prioritized for transmission to the MetroCard System. Since transactions are processed locally at the subway turnstile or IFU, whenever the MetroCard is swiped for entry to the subway or dipped for entry on to a bus the value of the MetroCard is read and the new value is written, but swiped or dipped cards are not validated in real-time against the central database. Several functions are performed at the individual readers, including risk management via storage of a Negative List, MetroCard

authorization, application of fare rules (e.g., recognizing transfers, unlimited ride passes), additions of value or time and reduction of a value-based card's available balance.

The MTA also advised that its "customers' personal data is only collected by our payment system as part of credit/debit authorization/sale transactions and not the usage transactions referenced in the response above."

The Metropolitan Transportation Commission stated:

> Patrons may register on the Clipper® Web Site or via their employer to establish a payment related account. Customer information retained may include name, contact information, and funding source information, such as a credit card or employer program. The information is retained on a secure back-office server and retained until an account is closed. Customer travel transactions do not contain personal information, but are recorded with the card account number within the transaction. This data is retained for up to 4.5 years, and then is purged to comply with CA State Law, to remove travel patterns.

The Milwaukee County Transit System reported that its customers currently may

> choose to order a card or register their smart card on the revaluing portal. Customers must provide an email address, name and address to do so in both cases. The information is housed in the backend system provided by the fare system vendor and only used to assist with customer service calls related to the card and account or to fulfill the card order.
>
> There is also a card history associated with each card that records interactions with sales outlet devices, handheld devices, the internet revaluing portal and the fare box. The device ID and time of the transactions are recorded and can be accessed by customer service representatives and also the customer if he/she has registered the card. In some special cases under agreements within existing programs, other information such as employer, age or disability status is also collected as part of program eligibility and tied to a specific smart card number. In most of those cases, a photo ID is also printed on to the card which is assigned to the successful program applicant under the terms and conditions of each program.
>
> MCTS also uses fare box card touches to monitor ridership, however that information is not used or monitored on an individual smart card basis, except at the request of law enforcement officials in the investigation of a case.

The Port Authority of Allegheny County stated:

> If a customer chooses to register their smart card for balance protection, we collect the customer's name, address, phone number. They answer 3 secret questions and enter the smart card chip ID. If they make a web purchase, we collect their credit card type, number, expiration date and billing address. The system collects what vehicle, date and time the smart card was tapped, but only associates the card with the user if registered. If the customer unlinks the card or closes their account, the user data for that card is no longer retrievable.

The Regional Transportation District explained that for contactless fare media (Smart Media), per Data Dictionary dated 8/9/2011, the system collects:

- Information on customers, web sales, and information collected through the customer call center. Includes but is not limited to:
  - Name
  - Maiden Name
  - Picture
  - Preferred title (Mr., Miss, etc.)
  - Sponsor ID
  - Rider Identification (for Students, this is their college/university Student ID)
  - Full address
  - Phone/alternative phone
  - Email
  - Web user ID/ password
  - Links to affiliated organization(s) IDs/contracts (school, neighborhood, etc.) as relates to the pass contract

- This data is furthermore linked to other data via the card serial number and/or profile, such as:
  - Card history and status
  - A record of transactions/inspections
  - Information on payment and transaction authorization, including encrypted bank card information

The District stated that the Web payment system for the contactless fare media is staged but not yet operational. While the transaction method is electronic, these systems generate paper media for use on vehicles.

For the static/mobile sales outlets and vending machines, when a credit card is used, the system records transaction data including the encrypted card number, patron name, etc. as relevant to the card transaction. Systems do not otherwise require user registration or data. Personal data is not captured electronically within these systems when cash is used.

Vendor operated websites may collect personal data to facilitate credit card transactions which can be traced to the patron's purchases (ex. a regional ticket book was purchased by [person with x card data] on [date]). The vendor manages the authentication method and transaction data and RTD is provided with reports.

Other agencies responding to the survey provided a brief description of their practice.[791]

[791] Central Florida Regional Transportation Authority (name, address, and last four digits of card only); City of Visalia Transit Department (collect travel information for some transactions and personal information); Connecticut Department of Transportation (credit and debit card information); Greater Cleveland Regional Transportation Authority (stating that for the Web store, a customer account registration process is required, a

4. Is your agency planning to adopt a new electronic payment system or systems?

(please circle) YES NO

Twenty-one agencies answered "Yes" to the question.[792] Thirteen agencies said "No."[793]

Orca stated: Planning phase has just started to determine the next generation ORCA system. We assume an account base system with open architecture but we are in the exploratory phase.

If your answer is "Yes," please describe:

(a) the system being adopted or that is under consideration for adoption; and

The Capital Area Transportation Authority referred to a Mobile fare-payment system: "We do not currently have details on the proposed system, other than to say that we are exploring all options regarding current and future payment systems, including but not limited to mobile payments, smart media and contactless media."

The Greater Cleveland Regional Transportation Authority identified a pilot for a mobile ticketing solution and software as a cloud-based service. "No data would be stored by GCRTA, as the user would create an account through their mobile phone."

---

customer mailing address is necessary, and that customer credit card information can be captured and stored per the customer's discretion); Laketran (smart card collects travel data); Lane Transit District (stating that customers have option of creating a user account on the District's Web site; that customers can provide their name, address, phone number, email address, and favorite routes; and that customers can elect to store their payment information for purchase of products through the District's Web store); Manchester Transit Authority (payment processed online and fare media mailed to customer; once completed, no information stored by MTA); Metra (TBI–name and mailing address; Mobile ticketing–email address, name, and birthdate); Orca (identifying usage data (trip, transfer) and fare acquisition data (card purchase and add value transactions) and data specific to eligibility for reduced fare ORCA cards); and Salem Area Mass Transit District (stating that the only data the agency collects are trip origin, bus route, date, and time, and that for consecutive trips occurring within a normal transfer window, it is assumed that a transfer occurred).

[792] Capital Area Transportation Authority, Central Florida Regional Transportation Authority, City of Madison Metro Transit,* City of Raleigh,* City of Visalia, Connecticut Department of Transportation, CT Transit,* Greater Cleveland Regional Transit Authority, Greater Lynchburg Transit Company,* Lane Transit District, Metra, Metropolitan Transportation Authority, Metropolitan Transportation Commission, Niagara Frontier Transportation Authority,* OmniTrans, ORCA Regional Coordination Program, Regional Transportation District, Salem-Keizer Transit, TriMet, Valley Regional Transit, and VIA Metropolitan Transit.

[793] Berkshire Regional Transit Authority, Capital Area Transportation Authority, Cobb Community Transit, Greater Hartford Transit District,* Laketran, Manchester Transit Authority, Metro Regional Transit Authority, Milwaukee County Transit System, Municipality of Anchorage Public Transportation Department, Port Authority of Allegheny County, Space Coast Area Transit, Sunline Transit Agency, and Topeka Metropolitan Transit Authority.

The Lane Transit District stated that the District "is considering use of a mobile ticket payment system and a fare card system utilizing smartcard technology. We anticipate that the system will use both closed-payment and open-payment methodologies."

According to the Metropolitan Transportation Authority, "[a]n RFP will be released shortly for an Account-Based, Open Payment architecture with Interfaces based on APIs provided by the SI (or its licensors). The New Fare Payments System shall include:

- Acceptance of Contactless Bank Cards, certain Third Party-Issued Media, MTA/NYCT-Issued Media, and other Media for fare payments via a range of channels, utilizing the appropriate security protocols.

- The NFPS Backend, an Account-Based Transaction Processor that manages Transit Accounts, calculates fare payments based on established Business Rules, handles all transaction processing (sales and usage) as appropriate, manages devices, provides Data for reporting to the Data Warehouse, and other such central data services.

- Real-time or near real-time communication Interfaces for all NFPS Equipment to the NFPS Backend.

- Extended-Use Smart Cards, operating as Account-Based Media.

- Limited-Use Smart Cards, operating as Account-Based or Card-Based Media.

- Bus Validators which shall accept all Media noted above and be mounted on vehicles as appropriate.

- Subway Validators which shall accept all Media noted above, and shall be installed within existing MTA/NYCT Faregates along with any equipment needed to control all Faregate functions for non-MetroCard transactions during the transition period and post-MetroCard decommissioning.

- Wayside Validator Machines which shall print receipts, accept all Media noted above and coin payments, and shall be installed next to SBS bus stops.

- Configurable Vending Machines to provide self-service kiosks to purchase MTA/NYCT-Issued Media, and to reload Fare Products in Closed-Loop Transit Accounts.

- Cash processing, reconciliation, reporting, inventory control and material handling cash settlement Software to support money room operations.

- A configurable Customer Service POS Terminal to provide sales, reload, registration, personalization (custom printing), and support and administrative functions for Transit Accounts and Media.

- A Customer Relationship Management System that allows for the central management of all Customer Data, and cradle-to-grave tracking of customer service tickets, including creation, escalation and resolution.

- A robust Fare Control Area Local Area Network to support communications between station Frontend NFPS Equipment and the NFPS Backend and NFPS Back Office via the MTA/NYCT network.

- The NFPS Websites to allow customers, institutions participating in Special Programs, Retail Merchants and MTA/NYCT staff to interact with the NFPS Backend for account management and other purposes.

- The NFPS Mobile Applications available on a range of operating systems for Customer Account management and payment purposes.

- Flexible and configurable reporting capability to provide comprehensive information to stakeholders in real-time or near-real-time as appropriate.

- Robust security, data redundancy, risk mitigation and fraud protection mechanisms.

- A Financial Clearing and Settlement System to provide revenue reconciliation and the settlement of funds between all Participating Agencies.

- A Data Warehouse to store NFPS Data for reporting, NFPS Back Office processing and monitoring purposes.

- Other services and support systems as described herein and as necessary for a modern fare collection system, including a Device Monitoring System and APIs to interface with other MTA/NYCT applications and processes (through MTA/NYCT-provided Interface Engines) as needed.

The Metropolitan Transportation Commission stated that its "Clipper® systems are being evaluated for replacement at the end of the current vendor contract. Requirements are still under development."

The Regional Transportation District said the agency is considering deploying mobile (smartphone) ticketing within the next 2 years; thus, it can be assumed that personal data will be collected as needed to facilitate financial and operational (ride approval and inspection) transactions.

Other agencies described briefly what they are considering.[794]

[794] Central Florida Regional Transportation Authority (mobile payment system/mobile phone application); City of Madison Metro Transit (implementation of system under development; recently purchased SPX/Genfare Fast Fare equipment); City of Raleigh, GoRaleigh (smart cards only); City of Visalia Transit Department (considering mobile ticketing system); Connecticut Department of Transportation (in early stages of discussing the implementation of smart cards as a means to pay for fares); CT Transit (smart card); Greater Lynchburg Transit Company (Genfare Smart Card system, contracted service); Metra (migrating TBI and CCTVM to utilize Bank of America Payeezy); Niagara Frontier Transportation Authority (an account-based contactless card system);

(b) the types of data that your agency will be collecting with the new system.

The Capital Area Transportation Authority reported that "[n]o details are available at this time, except that CATA will consider what data to collect in consideration of federal and state laws, as well as CATA's internal policies."

However, the Metropolitan Transportation Authority explained:

> The NFPS will collect sales & usage data, system performance data, equipment performance/maintenance data, customer data (including personal info and journey info. The NFPS will use a Tokenization process that meets or exceeds PCI Tokenization guidelines, and a certified Point-to-Point Encryption solution for all Payment Data. The Tokenization and encryption solutions will alleviate the need to store, and will allow secure processing of, Payment Data within the NFPS. The NFPS shall also ensure data security to the greatest extent possible.

Other agencies reported as described in the note.[795]

5. With your current or proposed electronic payment system are customers able:

(a) To use their credit and debit cards to pay for transit?

(please circle) YES NO

Twenty-three agencies answered "Yes" to the question.[796]

Omnitrans (mobile ticketing and/or smart card); Salem Area Mass Transit District (considering the use of open payment systems but agency is only in the exploration and evaluation stage); TriMet (considering an electronic fare system with contactless validators on both bus and rail; will be an account-based system featuring fare capping and open payments); and Via Metropolitan Transit (smart card system but not until 2017).

[795] Central Florida Regional Transportation Authority (name and address for delivery and last four digits of card); City of Madison Metro Transit (minimum data necessary for fare payment); Greater Cleveland Regional Transportation Authority (stating that only a customer's phone number is required); Greater Lynchburg Transit Company (ridership data but no financial data, all third-party managed); Lane Transit District (Trip origin (boarding) and trip destination (exit) data, pass program participation, and fare type usage); Metra (old system, different payment gateway); Metropolitan Transportation Commission (not yet determined).

[796] Berkshire Regional Transit Authority, Capital Area Transportation Authority, Capital District Transportation Authority, Central Florida Regional Transportation Authority, City of Raleigh,* City of Visalia, Connecticut Department of Transportation, CT Transit,* Greater Cleveland Regional Transit Authority, Greater Lynchburg Transit Company,* Laketran, Lane Transit District, Manchester Transit Authority, Metra, Metro Regional Transit Authority, Metropolitan Transportation Authority, Metropolitan Transportation Commission, Milwaukee County Transit System, OmniTrans, Port Authority of Allegheny County, Space Coast Area Transit, TriMet, and VIA Metropolitan Transit.

Nine agencies answered "No" to the question.[797]

If your answer is "Yes" to question 5(a), please provide details.

The Capital District Transportation Authority reported that a customer may

> use their credit or debit card on CDTA's website or in person at a point of sale terminal to purchase products or add value to existing products on their smart card. Electronic payment with a credit card cannot be performed on a transit vehicle. In the future, customer will be able to pay with a credit card via a mobile application or mobile ticket.

The Lane Transit District reported that all "credit and debit card transactions are processed for the District by PCI DSSI compliant vendors. Customer payment information is actually stored with a PCI DSS-compliant payment gateway service provider. The District's site stores an anonymous Payment ID value within the customer's web site profile for purchases though the District's web store."

The Metropolitan Transit Authority advised that currently credit and debit cards may be used at MetroCard Vending Machines, MetroCard Express Machines, and through the EasyPay Program, as well as in connection with the following commuter rail ticketing options.

LIRR has four types of Ticket Machines that sell MetroCards at their stations:

- Gray "Tickets" machines are full-service machines, selling most LIRR ticket types and pre-valued MetroCards. The following options are available: separate $25 MetroCard ($1 Green Fee applies), $5.50 MetroCard printed on the reverse side for Round Trip rail tickets, and $50 MetroCard printed on the reverse side for Monthly rail tickets. These machines accept cash as well as ATM/debit and credit cards.

- Red "Daily Tickets" machines sell One-Way and Round-Trip tickets and a separate $25 pre-valued MetroCard ($1 Green Fee applies) only. These machines accept cash as well as ATM/debit and credit cards.

- Blue "Tickets–Credit/Debit/ATM Cards" machines sell most LIRR ticket types and pre-valued MetroCard. The following options are available: separate $25 MetroCard ($1 Green Fee applies), $5.50 MetroCard printed on the reverse side for Round Trip rail tickets, and $50 MetroCard printed on the reverse side for Monthly rail tickets. These machines accept ATM/debit and credit cards only.

- Green "Tickets–AirTrain" machines sell most LIRR ticket types and offer $5 AirTrain MetroCards. These machines accept cash as well as ATM/debit and credit cards.

MNR has two types of Ticket Machines that sell MetroCards at their stations:

---

[797] Cobb Community Transit, Municipality of Anchorage, Public Transportation Department, Niagara Frontier Transportation Authority,* ORCA Regional Coordination Program, Regional Transportation District, Salem-Keizer Transit, Sunline Transit Agency, Topeka Metropolitan Transit Authority, and Valley Regional Transit.

- Gray "Tickets" machines are full-service machines, selling most MNR ticket types and pre-valued MetroCards. The following options are available: separate $25 MetroCard ($1 Green Fee applies), $5.50 MetroCard printed on the reverse side for Round Trip rail tickets, and $50 MetroCard printed on the reverse side for Monthly rail tickets. These machines accept cash as well as ATM/debit and credit cards.

- Red "Daily Tickets" machines sell One-Way and Round-Trip tickets and a separate $25 pre-valued MetroCard ($1 Green Fee applies) only. These machines accept cash as well as ATM/debit and credit cards.

The MTA further explained that

> [a]ll data tied to MetroCard usage and sales and credit/debit authorization requests are transmitted via a station controller which stores the information locally if communications are not available, in batched transmissions at timed intervals from vending machines, station booth terminal or turnstiles. Several key data components have higher priorities in the MetroCard System and are uploaded as soon as they arrive. These include authorization requests associated with credit/debit sales at vending machines and the backend portion of the MetroCard System that tracks credit/debit confirmations.

As for what is proposed, "credit and debit cards will be used to pay for fares at Vending Machines, through a customer Website, through mobile phones, and directly at the point of entry via readers on turnstiles and validators on board buses." *See also* MTA's answer to question 4(a).

The Metropolitan Transportation Commission reported that

> [p]atrons can use credit cards to fund a closed loop NFC card. Funds may be added at Ticket Vending Machine, Transit Office Terminal, or via the Web Site. These transactions are processed via a payment gateway maintained by the Clipper® primary contractor, acting as merchant on behalf of MTC or by one of the participating transit operators.

As for the Milwaukee County Transit System,

> [c]ustomers can use an online purchasing portal to buy fare products, which eventually get loaded onto a smartcard via a field device (usually a fare box on a bus). Sales outlets outfitted with Smart Media Attended Revaluing Devices also allow customers to pay with credit/debit, however it is up to the sales outlet to process those payments separate from the MCTS system.

According to the Port Authority of Allegheny County, customers may "use their credit cards at the ticket vending machines, sales office terminals at the Service Center, or on the web portal to purchase stored value or passes on their smart card." However, customers may not "tap their credit cards to fareboxes or validators and pay for individual rides."

The Regional Transportation District stated that

> [c]ustomers can use credit cards to purchase paper media at vendor websites, most vending machines, and all static/mobile sales outlets. Customers can use credit cards to pay for smart media transactions. In the near future, customers will be able to use their credit cards to pay for Smart Media associated fees and to add value to their Smart Media via website.

Other agencies also described their electronic payment systems.[798]

(b) To use Near Field Communications (NFC)-enabled mobile phones or other mobile devices to pay for transit?

(please circle) YES NO

Eight answered "Yes" to the question.[799] However, 22 answered "No."[800]

If your answer is "Yes" to question 5(b), please provide details.

The Capital District Transportation Authority stated that "[i]n the future, customers will be able to purchase products through a mobile application (mobile ticket) from an iOS or Android device. Once purchased, the customer would scan a 2D bar code of the mobile ticket on the farebox on the transit vehicle."

The Metropolitan Transportation Authority said that "NFC devices are one of the media types to be supported by the new NFPS system."

---

[798] Berkshire Regional Transit Authority (credit card accepted for payment at ticket vending machines and sale outlet terminals only); Capital Area Transportation Authority (stating that fare payment for online pass purchases at cata.org and in person at any number of points of sale); Central Florida Regional Transportation Authority (purchase bus pass via online or phone call, Web site uses pass through portal, and call-in direct to Bank of American merchant services); City of Raleigh, GoRaleigh (at ticket vending machines and current ticket outlets only); City of Visalia Transit Department (can purchase passes, make advance reservations, and pay by credit on some vehicles); Connecticut Department of Transportation (credit and debit cards accepted at ticket vending and machines and kiosks); CT Transit (not at farebox; only at sales outlets); Laketran (stating that transit passes/rides can only be purchased online with a credit or debit card and that customers must pay cash or use a smart card to pay for bus rides); Manchester Transit Authority (credit cards can be used online or in person at MTA office; not useable on vehicles or at bus stops); Metra (Mobile ticketing, TBI, CCTVM, and POS); Metro Regional Transit Authority (stating that credit card can be used to purchase fare media at customer service center); and Omnitrans (indirectly, i.e., vending machine or on line store purchases).

[799] Central Florida Regional Transportation Authority, City of Visalia, Greater Lynchburg Transit Company,* Lane Transit District, Metra, Metropolitan Transportation Authority, Salem-Keizer Transit, and TriMet.

[800] Berkshire Regional Transit Authority, Capital Area Transportation Authority, Capital District Transportation Authority, City of Raleigh,* Cobb Community Transit, Connecticut Department of Transportation, Greater Cleveland Regional Transit Authority, Laketran, Manchester Transit Authority, Metropolitan Transportation Commission, Milwaukee County Transit System, Municipality of Anchorage, Public Transportation Department, Niagara Frontier Transportation Authority,* OmniTrans, ORCA Regional Coordination Program, Port Authority of Allegheny County, Regional Transportation District, Space Coast Area Transit, Sunline Transit Agency, Topeka Metropolitan Transit Authority, Valley Regional Transit, and VIA Metropolitan Transit.

Other agencies also provided information.[801]

6. If your agency is using customers' personal data, please describe how the data is being used:

a) For the benefit of the agency:

The Capital District Transportation Authority advised that the limited personal information is used to support customer account management of product purchases and account balances as well as to understand travel usage and ridership trends.

The Lane Transit District "retains basic personal data, as identified above, for the express purpose of conducting business with our customers. Customers can agree to receive supplemental District-related information by subscribing to topic lists through their web profile. The District does not share its customer information."

The Metropolitan Transportation Authority uses the data "[t]o facilitate convenient, secure, and efficient fare collection. We will also be using the data to be able to provide an enhanced level of customer service, including self-service options, that requires the collection and use of personal data to set-up, administer, and manage customer accounts."

For the Metropolitan Transportation Commission "[p]ersonal data is used to process business transactions, such as payments, refunds or customer service questions. In the case of patrons who opt in to receive communications, email or mailing addresses may be used to inform patrons of transit related information updates (e.g., fare changes, etc.)."

Overall, the Milwaukee County Transit System,

> uses smart card activity to track ridership; however, that is not done on an individual basis. On a customer/individual level, customer service can access registered cardholder information to help ensure that the individual calling is the actual cardholder. In this way it helps limit fraud, or potential fraud, by requiring the customer to prove they are the rightful cardholder before MCTS credits any value that has been lost or stolen.

Other agencies also provided information.[802]

---

[801] Central Florida Regional Transportation Authority (mobile payment system); City of Visalia Transit Department (can only use to purchase passes in transit office; contactless); Lane Transit District (currently considering options for fare payment via mobile devices, a service not being provided at the present); and Metra (mobile application for tickets).

[802] Central Florida Regional Transportation Authority (to try and identify charge backs via last four numbers on card); City of Visalia Transit Department (demographic reports); Greater Cleveland Regional Transportation Authority (customer e-mail notification of special offers and products); Laketran (travel can be tracked through a smartcard that is associated with a card number assigned to that person); ORCA (stating that personal data is currently not used unless in the investigation of fraud or other crime); Port Authority of Allegheny County (stating that customers' personal data are not used for the agency's benefit; Salem Area Mass Transit District (using travel data to assist with system planning and determining allocation of resources to enhance efficiencies in operation); TriMet (studying demographics, generalized ridership patterns to plan better service, routing, frequency and other customer experience benefits); and Regional Transportation District (for identification

b) For the benefit of customers:

The Capital District Transportation Authority stated:

> Customers' personal information is used to identify unique account information and protect customers against fraudulent account transactions. In other words, it is used to validate the customer's identity during a customer service call with a CDTA account representative. The customer's electronic mail address is used to validate account creation and modifications, and provide customers with the ability to manage their account balance on their own. The customer's address information is used to enable the shipment of new media or products. The customers' credit card information is used to process payment transactions. Only the last 4 digits of their credit card number is available to help with a payment processing question.

According to the Metropolitan Transportation Commission, the benefits are "[t]o facilitate convenient, secure and efficient fare collection and to be able to provide an enhanced level of customer service, including self-service options, that requires the collection and use of personal data to set-up, administer, and manage customer accounts."

Benefits reported by the Milwaukee County Transit System are that "[b]y registering a smartcard with the agency, [the] MCTS will replace any lost electronic fare value if a card is lost or stolen. This requires name, address and email and phone number data to be provided."

The Port Authority of Allegheny County stated that "[c]ustomers may be contacted by the Authority to communicate important system changes or to provide information about their Smart Card and products if required. Customer Service will contact customers if they have called in with a complaint with remediation information or to follow up on a complaint investigation."

Other agencies provided information on what they regarded as customer benefits.[803]

---

purposes (*e.g.,* links card to the owner of the card, owners to contracts, and contract administrators so that the agency can provide program administration/customer service)).

[803] Central Florida Regional Transportation Authority (to identify customers for refunds and proper delivery addresses for products); City of Visalia Transit Department (confirm reservations for premium shuttle service); Greater Cleveland Regional Transportation Authority (customer email notification of special offers and products); Laketran (travel can be tracked through a smart card that is associated with a card number assigned to that person); Lane Transit District (stating that customers can receive personalized information about favorite routes, trips, and events and can conveniently purchase fare products through the District's Web store); ORCA (stating that personal data is currently not used unless in the investigation of fraud or other crime); Port Authority of Allegheny County (stating that customers' personal data are not used for the agency's benefit); Salem Area Mass Transit District (using travel data to assist with system planning and determining allocation of resources to enhance efficiencies in operation); TriMet (studying demographics, generalized ridership patterns to plan better service, routing, frequency, and other customer experience benefits); Regional Transportation District (stating for identification purposes (e.g., links card to the owner of the card, owners to contracts, contract administrators, so agency can provide program administration/customer service); Port Authority of Allegheny County (stating that customers' personal data are not used for the agency's benefit); Salem Area Mass Transit District (using travel data to assist with system planning and determining allocation of resources to enhance efficiencies in operation);

7. (a) Does your agency have an agreement, terms of use, and/or privacy policy that it uses in connection with its electronic payment system?

(please circle) YES NO

Fifteen agencies answered "Yes" to the question.[804] Eighteen agencies answered "No."[805]

If your answer is "Yes" to question 7(a), please provide a copy of or a link to any agreement(s), terms of use, and/or privacy policy that your agency uses.

The Metropolitan Transportation Authority provided copies of two policies: Enterprise Electronic Information Security Policy and Release of Electronic Customer Account Information. ORCA also provided a copy of its Terms of Use and Privacy Statement.

The links the agencies provided are set forth in the note.[806]

TriMet (studying demographics, generalized ridership patterns to plan better service, routing, frequency, and other customer experience benefits); Regional Transportation District (use for identification purposes, such as to link card to the owner of the card and for contract administrators so that the agency can provide program administration/customer service)).

[804] Capital Area Transportation Authority, Capital District Transportation Authority, Central Florida Regional Transportation Authority, City of Visalia, Greater Cleveland Regional Transit Authority, Lane Transit District, Metropolitan Transportation Authority, Metropolitan Transportation Commission, Milwaukee County Transit System, ORCA Regional Coordination Program, Port Authority of Allegheny County, Regional Transportation District, Topeka Metropolitan Transit Authority, TriMet, and VIA Metropolitan Transit.

[805] Berkshire Regional Transit Authority, City of Madison Metro Transit,* City of Raleigh,* Cobb Community Transit, Connecticut Department of Transportation, Greater Lynchburg Transit Company,* Laketran, Manchester Transit Authority, Metra, Metro Regional Transit Authority, Municipality of Anchorage, Public Transportation Department, Niagara Frontier Transportation Authority,* OmniTrans, Salem-Keizer Transit, Space Coast Area Transit, Sunline Transit Agency, Valley Regional Transit, and Westchester County Department of Public Works and Transportation.

[806] Capital Area Transportation Authority, (http://www.cata.org/popup.aspx?title=Privacy+Information&topic=privacy ; http://www.cata.org/Fares/BuyPassesOnline/tabid/212/buypassesonline/productdetails/tabid/314/p-37-commuter-lot-2nd-semester-pass.aspx and authorize.net, which has its own security suite for data-protection purposes; processes CATA's online orders); Capital District Transportation Authority (http://www.cdta.org/privacy-policy/94); Central Florida Regional Transportation Authority; City of Visalia Transit Department (managed through city's finance department); Connecticut Department of Transportation (http://cttransit.com/PrivacyPolicy/ and http://web.mta.info/mta/privacy.htm); Greater Cleveland Regional Transportation Authority; Lane Transit District (https://www.ltd.org/privacy-policy/); Metropolitan Transportation Commission (https://www.clippercard.com/clipperWeb/privacy.do) Milwaukee County Transit System (http://www.ridemcts.com/fares-passes/m-card-privacy-policy and http://www.ridemcts.com/fares-passes/m-card-terms-and-conditions); Port Authority of Allegheny County (http://connectcard.org/media/5979/connectcard_termsconditions.pdf and http://connectcard.org/media/5976/ConnectCard_PrivacyPolicy.pdf); and Regional Transportation District (http://www.rtd-denver.com/Privacy_Policy.shtml , http://www.rtd-denver.com/TermsofUse.shtml, and http://www.rtd-denver.com/SM_Privacy.shtml).

(b) Does your agency have a website that collects customers' personal data when they use the website?

(please circle) YES NO

Sixteen answered "Yes" to the question.[807] Seventeen agencies answered "No."[808]

If your answer is "Yes" to question 7(b), please provide a copy of or a link to any agreement, terms of use, and/or privacy policy that your agency uses for the website.

The Metropolitan Transportation Authority attached a copy of its Internet Privacy Policy.

The Milwaukee County Transit System stated that when the agency introduced the online revaluing portal, the terms and policies were also reviewed and updated for the RideMCTS.com website by third party legal counsel. ORCA also provided a copy of its Terms of Use and Privacy Statement.[809]

8. (a) If not answered by the agreements, terms of use, and privacy policy or policies provided in response to question 7(a) and/or 7(b), please state:

(1) Who owns the personal data collected by your agency?

As did several other agencies, the Capital Area Transportation Authority reported that any information collected by CATA is owned by CATA exclusively.[810] As did several other agencies, the Metropolitan Transportation Authority stated that the relevant information is addressed in its policies.[811]

---

[807] Capital Area Transportation Authority, Capital District Transportation Authority, City of Visalia, CT Transit,* Greater Cleveland Regional Transit Authority, Laketran, Lane Transit District, Metro Regional Transit Authority, Metropolitan Transportation Authority, Metropolitan Transportation Commission, Milwaukee County Transit System, ORCA Regional Coordination Program, Port Authority of Allegheny County, Regional Transportation District, TriMet, and VIA Metropolitan Transit.

[808] Berkshire Regional Transit Authority, Central Florida Regional Transportation Authority, City of Madison Metro Transit,* City of Raleigh,* Cobb Community Transit, Greater Hartford Transit District,* Greater Lynchburg Transit Company,* Manchester Transit Authority, Municipality of Anchorage, Public Transportation Department, Niagara Frontier Transportation Authority,* OmniTrans, Salem-Keizer Transit, Space Coast Area Transit, Sunline Transit Agency, Topeka Metropolitan Transit Authority, Valley Regional Transit, and Westchester County Department of Public Works and Transportation.

[809] Other agencies responded as follows: Greater Cleveland Regional Transportation Authority (stating that neither exists); Lane Transit District (https://www.ltd.org/privacy-policy/); and Metro Regional Transit Authority (stating that policy at www.akronmetro.org/metro_enews.aspx is limited to the following: "We don' t share your email address with any third parties and you can unsubscribe anytime by coming back to this page.").

[810] City of Visalia Transit Department (the City); Laketran (the agency owns data); Lane Transit District (stating that the District owns all personal data collected on the Web site); Port Authority of Allegheny County (stating that the Authority is the sole owner); and Salem Area Mass Transit District (travel data owned by the District).

[811] Capital Area Transportation Authority (http://www.cata.org/popup.aspx?title=Privacy+Information&topic=privacy); Capital District Transportation Authority (http://www.cdta.org/privacy-policy/94); Connecticut Department of Transportation (stating that the

Several other agencies noted that they do not retain data.[812]

(2) Who has access to the personal data?

The Capital District Transportation Authority stated:

> Personal data are available for sales purposes. The Sales and Finance departments have access to this data. Lane Transit District stated: Authorized District personnel and authorized third-party contractors supporting the District's web site. The District maintains the authorization credentials.

The Metropolitan Transportation Commission stated that the contractor who manages the program on behalf of the agency and participating transit operators has access to the data.

According to the Milwaukee County Transit System, its Web site is hosted by a third part agency; access is a combination of MCTS and the agency that uses the information for marketing purposes.

The Port Authority of Allegheny County reported that the

> Port Authority Automated Fare Collection System (AFCS) Administrators and Customer Service representatives and agents have access to customer information. Regional Transit Agency Partners (Butler Transit Authority, Fayette Area Coordinated Transit, Mid Mon Valley Transit Authority, Westmoreland Transit Authority and Washington Freedom Transit) Customer Service Representatives have access to look up registered card user data when providing customer service.

Other agencies responding to the survey provided information regarding who has access to data.[813]

---

following links have the State of Connecticut Internet Access and Privacy policies as well as the Connecticut Personal Data Act, http://www.access.state.ct.us/policies/accesspolicy40.html ; http://portal.ct.gov/policies/state-privacy-policy/ ; http://portal.ct.gov/policies/computer-personal-data-act/); CT Transit (see privacy policy at www.CTTransit.com); Metropolitan Transportation Commission (https://www.clippercard.com/clipperWeb/privacy.do); http://www.ridemcts.com/Privacy-Statement/; and http://www.ridemcts.com/terms-of-use/); Port Authority of Allegheny County (http://connectcard.org/media/5976/ConnectCard_PrivacyPolicy.pdf); and Regional Transportation District (http://www.rtd-denver.com/Privacy_Policy.shtml, http://www.rtd-denver.com/TermsofUse.shtml, and http://www.rtd-denver.com/SM_Privacy.shtml).

[812] Central Florida Regional Transportation Authority (LYNX does not retain payment data, only last four digits of card); and Manchester Transit Authority (MTA has a Web site but no personal data is collected; payment processed by a third party and then data deleted).

[813] Berkshire Regional Transit Authority (not collected); Capital Area Transportation Authority (see Privacy and Security standards, http://www.cata.org/popup.aspx?title=Privacy+Information&topic=privacy ; Central Florida Regional Transportation Authority (only personnel that have a need based upon requirements–customer service and revenue technicians); City of Visalia Transit Department (select staff members, city employees (not all), and marketing firm); Greater Cleveland Regional Transportation Authority (information stored in-house within

(3) What personal data may be accessed and under what circumstances?

The Metropolitan Transportation Commission stated that

> [p]ersonal data may be accessed only by employees of MTC, MTC's contractors, participating operators, and by the patron themselves under specifically designed controls and business processes that vary by action. All individuals who receive access are managed by audited access controls operated by the contractor. Access by additional parties is restricted in compliance with applicable state law.

The Milwaukee County Transit System has an opt-in rider benefits program that also includes email updates and communication. The MCTS collects contact information and other ridership and demographic information as part of that optional sign up.

The Port Authority of Allegheny County stated:

> The customer's name, address, contact information, smart card number and smart card usage can be viewed by Customer Service Representatives and AFCS Administrators on an individual basis when investigating complaints. A database query to list all customers is only accessible to Port Authority IT Database Administrators.

Other responding agencies also provided information.[814]

(4) How long may data be retained, stored, or archived?

Agencies' answers varied in response to the question. For example, the Capital Area Transportation Authority advised that there is no expressed limit to the best of its knowledge.

The Capital District Transportation Authority reported that "[d]ata are retained for customer accounts that remain active. Inactive accounts are purged after 12 months."

GCRTA); Laketran (only the agency); Metro Regional Transit Authority (communication department at METRO); and Salem Area Mass Transit District (only district planning and IT staff).

[814] Capital Area Transportation Authority (Privacy and Security, http://www.cata.org/popup.aspx?title=Privacy+Information&topic=privacy); Central Florida Regional Transportation Authority (name and address for delivery confirmation; possible identification of charge backs, refunds); City of Visalia Transit Department (name, address, phone, email, and pass number); Greater Cleveland Regional Transportation Authority (customer address required for shipment of fare media purchases); Laketran (order history, billing and shipping details, email, phone, and username for online account, but only used internally to manage payment process); Lane Transit District (stating that authorized parties, as previously described, have access to the personal data stored on the District's Web site); Metro Regional Transit Authority (only name and email address for newsletter); and Salem Area Mass Transit District (only travel data that is accessed on a monthly basis for analysis and generation of performance reports).

The Lane Transit District said that "[p]ersonal data is currently stored in perpetuity by the District's web site hosting provider. Plans for automated archiving of the data are not defined at this time."

The Milwaukee County Transit System stated that it "recently began a contract with a new third party agency who will be maintaining and hosting the RideMCTS.com website so this is currently unknown."

According to the Port Authority of Allegheny County,

> [c]ustomer data for registered accounts is saved for as long as a customer maintains the account. It is only used to process their transactions. Transaction data is only kept for 14 months in the primary system. All transactions are archived nightly to the data warehouse. This information does NOT include credit card data. We do record the payment method and amount, but the data warehouse does not keep the credit card information.

Other agencies' answers are reported in the note.[815]

(5) What safeguards are used to prevent hacking and misuse of customers' personal data?

The Capital Area Transportation Authority stated:

> We take reasonable precautions to protect your information. For example, we encrypt certain communications through our website with 128-bit encryption, the industry standard for strong encryption. However, given the nature of the Internet and the fact that network security measures are not infallible, we cannot guarantee the security of visitors' information.

Capital District Transportation Authority reported that

> [t]he use of secure communications (SSL) with no direct access to data sources except through web based applications, and the use of strong password enforcement for login and account access are the primary safeguards used to prevent hacking and misuse.

The Lane Transit District said that its

---

[815] Central Florida Regional Transportation Authority (indefinite; remains until removed); City of Visalia Transit Department (unknown); Greater Cleveland Regional Transportation Authority (retention has not been established); Laketran (purchase orders–forever; credit card data–never); Manchester Transit Authority (no data retained); Metro Regional Transit Authority (information kept until email is no longer valid or patron asks to be removed); Salem Area Mass Transit District (travel data for many years to compare performance trends from year to year); and TriMet (currently varies on purpose (generally 3 years), e-fare up to 8 years to comply with applicable retention laws).

web site has basic restrictions for creating a user profile password. The District's web site host provider has server monitoring and high standards for credentialed access by their staff to all servers. The hosting provider restricts remote access to servers to credentialed administrators only.

The Metro Regional Transit Authority advised that "[i]nformation is stored at a third party vendor and we do not have direct knowledge of how they secure the email addresses."

The Metropolitan Transportation Commission has "a comprehensive security architecture in place that is audited on an annual basis."

The Milwaukee County Transit System has begun "a contract with a new third party agency who will be maintaining and hosting the RideMCTS.com website so this is currently unknown to the full extent. So far efforts have been made to examine site security and update the SSL certificate."

All of the Port Authority of Allegheny County's "credit card information is encrypted in the database and on the device (either web server or TVM). The servers have a restricted access list of administrators who can access them. However, even a database administrator cannot read a credit card number from the database. Customer Service reps and other system users cannot see full credit card information."

Other agencies also provided information in response to the question.[816]

9. (a) Does your agency have an agreement with a contractor or agent (or other holder of customers' personal data) for the purpose of collecting, using, disclosing, and/or retaining data obtained by a contactless (or other) electronic payment system?

(please circle) YES NO

Ten agencies answered "Yes" to the question.[817] Twenty-three agencies answered "No."[818]

---

[816] Central Florida Regional Transportation Authority (information technology provides network security with data being collected through third-party portal); City of Visalia Transit Department (EV, SSL certifications, and contract with "DigiCert"); Greater Cleveland Regional Transportation Authority (information stored with the Oracle database, patched according to security as specified by Oracle); Laketran (user roles for internal safeguarding; SSL and TLS for secure connections); Manchester Transit Authority (network protected by City of Manchester Information Systems department); Salem Area Mass Transit District (stating that because there are no connections between the fare implement and the passenger's personal identity, there are no additional security protocols beyond standard district network security systems); and TriMet (anonymizing of data, security assessment by accredited industry professional, and adherence to latest payment standards).

[817] Central Florida Regional Transportation Authority, City of Visalia, Greater Cleveland Regional Transit Authority, Metra, Metropolitan Transportation Commission, Milwaukee County Transit System, OmniTrans, ORCA Regional Coordination Program, Port Authority of Allegheny County, and Regional Transportation District.

[818] Berkshire Regional Transit Authority, Capital Area Transportation Authority, Capital District Transportation Authority, City of Madison Metro Transit,* City of Raleigh,* Cobb Community Transit, CT Transit,* Greater Cleveland Regional Transit Authority, Greater Hartford Transit District, Greater Lynchburg Transit Company,*

If your answer is "Yes," please provide a copy of or a link to any such agreement or agreements.

Although not answering the question directly the Metropolitan Transportation Authority stated that "only as an incidental element of the core purpose of the agreement. Such agreements are subject to applicable privacy law and the appended policies."

The Metropolitan Transportation Commission stated that it "has a design, build, operate, and maintain contract agreement with Cubic Transportation Systems that addresses these items."

ORCA stated that pursuant to a contract, and in accordance with PCI standards and applicable laws, "Vix Technology is responsible for data collected by the fare payment system. The card data environment is segregated to define where PCI resides and how it flows through the system."

The Port Authority of Allegheny County stated that the "RTAs have a signed 'Fare System Interoperability Agreement' executed between the Port Authority and the five participating RTAs [that defines] the use and confidentiality of customer account information."

The Regional Transportation District's vendors' support of electronic fare systems under the "contract with RTD are governed by the terms of the contract, which may include confidentiality clauses. These vary by contract and may not directly address personally identifiable information."

Other agencies also provided information.[819]

(b) If not answered by your response to question 9(a), how does your agency describe or define the obligations of your agency, its contractor(s), or other holders of customers' personal data?

Although most information was provided in response to the previous question, the Lane Transit District reported that it and its "web site hosting vendor have discussed this subject and operate with a common understanding of intentions. There is no formal coverage of this issue in existing agreements between the District and its web site hosting vendor."[820]

10. Is your agency "monetizing" customers' personal data that the agency (or a contractor or agent on behalf of the agency) collects?

(please circle) YES NO

Laketran, Lane Transit District, Manchester Transit Authority, Metro Regional Transit Authority, Municipality of Anchorage, Public Transportation Department, Niagara Frontier Transportation Authority,* Salem-Keizer Transit, Space Coast Area Transit, Sunline Transit Agency, TriMet, Westchester County Department of Public Works and Transportation, and VIA Metropolitan Transit.

[819] Central Florida Regional Transportation Authority (Bank of America merchant services); Greater Cleveland Regional Transportation Authority (establishing one now for the mobile ticketing pilot only); and Laketran (stating that it will be adding soon to its Terms of Use policy in www.laketran.com).

[820] Greater Cleveland Regional Transportation Authority (no rules established); Metra (only as part of other agreements; nothing separate for customer data); and Metropolitan Transportation Commission (referring to its privacy policy, https://www.clippercard.com/clipperWeb/privacy.do).

No agency answered "Yes" to the question. Thirty-four answered "No" to the question.[821]

If your answer is "Yes," please describe the ways in which the agency is monetizing customers' personal data.

As noted, no agency answered "Yes" to the question.

11. Does your agency have any agreements with third-party developers that involve the sharing of customers' personal data for the purpose of offering customers certain benefits or options?

(please circle) YES NO

Only two agencies answered "Yes" to the question: Metra and TriMet. Thirty-one agencies answered "No."[822]

If your answer is "Yes," please provide details and/or a copy of or a link to any such agreement(s).

Metra identified its agreement with Cubic.

12. Are there any federal or state constitutional provisions, laws, regulations, or policies of which you are aware that apply to your agency's (or contractor's) collection, use, disclosure, or retention of customers' personal data?

(please circle) YES NO

---

[821] Berkshire Regional Transit Authority, Capital Area Transportation Authority, Capital District Transportation Authority, Central Florida Regional Transportation Authority, City of Madison Metro Transit,* City of Raleigh,* City of Visalia, Cobb Community Transit, Connecticut Department of Transportation, CT Transit,* Greater Cleveland Regional Transit Authority, Greater Hartford Transit District,* Greater Lynchburg Transit Company,* Laketran, Lane Transit District, Manchester Transit Authority, Metra, Metro Regional Transit Authority, Metropolitan Transportation Authority, Metropolitan Transportation Commission, Milwaukee County Transit System, Municipality of Anchorage, Public Transportation Department, Niagara Frontier Transportation Authority,* OmniTrans, ORCA Regional Coordination Program, Port Authority of Allegheny County, Regional Transportation District, Salem-Keizer Transit, Space Coast Area Transit, Sunline Transit Agency, Topeka Metropolitan Transit Authority, TriMet, Westchester County Department of Public Works and Transportation, and VIA Metropolitan Transit.

[822] Berkshire Regional Transit Authority, Capital Area Transportation Authority, Capital District Transportation Authority, Central Florida Regional Transportation Authority, City of Madison Metro Transit,* City of Raleigh,* City of Visalia, Cobb Community Transit, CT Transit,* Greater Hartford Transit District,* Greater Lynchburg Transit Company,* Laketran, Lane Transit District, Manchester Transit Authority, Metro Regional Transit Authority, Metropolitan Transportation Authority, Metropolitan Transportation Commission, Milwaukee County Transit System, Municipality of Anchorage, Public Transportation Department, Niagara Frontier Transportation Authority,* OmniTrans, ORCA Regional Coordination Program, Port Authority of Allegheny County, Regional Transportation District, Salem-Keizer Transit, Space Coast Area Transit, Sunline Transit Agency, Topeka Metropolitan Transit Authority, Valley Regional Transit, and Westchester County Department of Public Works and Transportation. VIA Metropolitan Transit did not respond to the question.

Eleven agencies answered "Yes" to the question.[823] Nineteen agencies answered "No."[824]

If your answer is "Yes," please identify and provide a copy of or a link to any such agreement or agreements.

The Metropolitan Transportation Commission identified the California Streets and Highways Code § 31490 but noted that the provision is "specific to our industry" and that "other standard Federal and California state merchant-related privacy law also applies."

The Niagara Frontier Transportation Authority referred to the Federal Trade Commission Act, New York State Personal Privacy Protection Law (Public Officer's Law, art. 6-A, §§ 91-99), New York State General Business Law § 899aa, and ISO 27001 (standard for best practices in operation).

ORCA cited the Washington State Public Records Act, Rev. Code Wash. § 42.56 and the Uniform Unclaimed Property Act, Rev. Code Wash. § 63.29.

The Regional Transportation District stated that depending on the definition of personal information, the nature of the request, and the requestor's identity, customer data may be disclosed under the Colorado Open Records Act (CORA). Furthermore, depending on the definition of personal information, the retention and disclosure of customer data may be limited under Colo. Rev. Stat. § 24-72-113 (Passive Surveillance).

Other laws that the agencies cited are included in the note.[825]

---

[823] Capital District Transportation Authority, Central Florida Regional Transportation Authority, Greater Hartford Transit District,* Manchester Transit Authority, Metra (Personal Information Act, 805 ILL. COMP. STAT. 530: Controlling the Assault of Non-Solicited Pornography and Marketing, 15 U.S.C. §§ 7701–7713; Electronic Mail Act, 815 ILL. COMP. STAT. 5111-15; and Identity Protection Act, 5 ILL. COMP. STAT. 179/1), Metropolitan Transportation Authority, Metropolitan Transportation Commission, ORCA Regional Coordination Program, Regional Transportation District, Space Coast Area Transit, and TriMet.

[824] Berkshire Regional Transit Authority, Capital Area Transportation Authority (but noting that this was not an area of the respondent's expertise), City of Madison Metro Transit,* City of Raleigh,* City of Visalia, Cobb Community Transit, Greater Cleveland Regional Transit Authority, Greater Lynchburg Transit Company,* Laketran, Lane Transit District, Metro Regional Transit Authority, Municipality of Anchorage, Public Transportation Department, Port Authority of Allegheny County, Salem-Keizer Transit, Sunline Transit Agency, Topeka Metropolitan Transit Authority, Valley Regional Transit, Westchester County Department of Public Works and Transportation, and VIA Metropolitan Transit. Milwaukee County Transit System and Niagara Frontier Transportation Authority did not response to the question.

[825] Capital District Transportation Authority (New York State Privacy Protection Law–http://www.dos.ny.gov/coog/shldno1.html); Central Florida Regional Transportation Authority (stating that the agency adheres to all of the Florida state retention provisions); CT Transit (identifying PCI DSS compliance); and Metra (identifying the Personal Information Protection Act, 805 ILL. COMP. STAT. 530; CAN-SPAM, 15 U.S.C. §§ 7701–7713; Electronic Mail Act, 815 ILL. COMP. STAT. 5111-15; and Identity Protection Act, 5 ILL. COMP. STAT. 179/1); TriMet (*citing* OR. REV. STAT. § 192.501(38) (regarding exemption of personally identifiable information collected as part of electronic fare)).

13. If your agency accepts payment for transit fares by credit or debit cards has your agency (or a contractor or agent on behalf of your agency) taken steps to comply with the Payment Card Industry Data Security Standards (PCI DSS)?

(please circle) YES NO

Twenty-five agencies answered "Yes" to the question.[826] Only five agencies answered "No."[827]

If your answer is "Yes," please provide details and/or a link to or a copy of any agreement(s) between your agency and any financial institution and/or any credit or debit card company regarding PCI DSS-compliance.

Capital District Transportation Authority stated that the

> [c]ontract language between the electronic fare payment system vendor and bank card processing service provider is available. In addition, the point of sale system is PA-DSS certified and the hosted web portals are Level 2 merchant status PCI certified. The SAQ A–EP certification is used for CDTA.

As for the Central Florida Regional Transportation Authority, its "point of sales program ensures compliance by adhering to all conditions as outlined in terms of network and resource security (merchant services).

The Greater Cleveland Regional Transportation Authority reported that the "completion and verification of the Authority's PCI compliance documentation is required for Hosted, Non-hosted and Network assessments/checklist for payment card processing service partners."

The Lane Transit District explained that its

> website hosting vendor contracts with a PCI DSSI compliant datacenter that provides commercial ecommerce hosting resources. All data relating to financial transactions between the District's web site services and financial institutions is transmitted directly to the District's PCI DSSI compliant payment gateway provider. The District and its web site hosting vendor do not retain any personal financial information.

---

[826] Berkshire Regional Transit Authority, Capital Area Transportation Authority, Capital District Transportation Authority, Central Florida Regional Transportation Authority, City of Raleigh,* City of Visalia, Connecticut Department of Transportation, CT Transit,* Greater Lynchburg Transit Company, Lane Transit District, Manchester Transit Authority, Metra, Metro Regional Transit Authority, Metropolitan Transportation Authority, Metropolitan Transportation Commission, Milwaukee County Transit System, Municipality of Anchorage, Public Transportation Department, OmniTrans, Port Authority of Allegheny County, Regional Transportation District, Salem-Keizer Transit, Sunline Transit Agency, TriMet, Valley Regional Transit, and VIA Metropolitan Transit.

[827] Cobb Community Transit, Greater Lynchburg Transit Company,* Laketran, Niagara Frontier Transportation Authority,* and ORCA Regional Coordination Program. Three agencies, Space Coast Area Transit, Topeka Metropolitan Transit Authority, and Westchester County Department of Public Works and Transportation, did not respond or were unsure.

The Metropolitan Transportation Commission's vendor makes the annual PCI DSS compliance certification.

The Milwaukee County Transit System's "fare collection system vendor hosts the online purchasing portal and the connection to the bank processor" and has "certified to us that they are and will remain PCI-DSS compliant."

The Regional Transportation District is a

> Level 2 Merchant under PCI-DSS and are applying PCI-DSS to all of our credit card processing systems. RTD is obligated to provide an Attestation of Compliance to our merchant bank annually. Vendors that accept payments on RTD's behalf or that host systems that are (wholly or in part) part of the credit-card processing data flow are required by contract to comply with PCI-DSS.

The Salem Area Mass Transit District "uses a virtual terminal solution for credit card processing. A virtual terminal is a web based credit card terminal accessed across a secure HTTPS connection. No credit card information is ever written down or stored at the district's facilities."

Other agencies also provided information.[828]

14. Within the past five years have there been any legal actions brought against your agency (or a contractor or agent of your agency):

(a) alleging a violation of a customer's right to privacy?

(please circle) YES NO

No agency responding to the survey answered "Yes" to the question. All others answered "No."[829]

---

[828] Berkshire Regional Transit Authority (stating that Scheidt and Bachman in the process of complying with PCI DSS and that the MBTA administers the project); Capital Area Transportation Authority (stating that authorize.net processes online orders and has its own security suite); City of Visalia Transit Department (managed through city's finance department); Laketran (stating that compliance not mandated; agency does not store credit card information); Manchester Transit Authority (bank processes payments and has certified compliance); Metra (stating that it uses vender control case for POS only but that the agency can provide certification document if needed); Port Authority of Allegheny County (providing copies PCI DSS-compliance agreements/documents with Bank of America and First Data Merchant Services); and Via Metropolitan Transit (compliance through its financial institution, Chase Paymentech, in regard to PCI DSS, PA-DSS, SDP, and CI5P).

[829] Berkshire Regional Transit Authority, Capital Area Transportation Authority, Capital District Transportation Authority, Central Florida Regional Transportation Authority, City of Madison Metro Transit,* City of Raleigh,* City of Visalia, Cobb Community Transit, Connecticut Department of Transportation, CT Transit,* Greater Cleveland Regional Transit Authority, Greater Hartford Transit District,* Greater Lynchburg Transit Company,* Laketran, Lane Transit District, Manchester Transit Authority, Metra, Metro Regional Transit Authority, Milwaukee County Transit System, Municipality of Anchorage, Public Transportation Department, Niagara Frontier Transportation Authority,* OmniTrans, ORCA Regional Coordination Program, Port Authority of Allegheny County, Regional Transportation District, Salem-Keizer Transit, Space Coast Area Transit, Sunline Transit Agency, TriMet, Valley Regional Transit, Westchester County Department of Public Works and

If your answer is "Yes," please provide details and a citation to any case(s) or decision(s).

(b) alleging that a customer's data was compromised because of a breach of security of their personal data?

(please circle) YES NO

No agency responded "Yes" to the question. All other agencies responding to the survey answered "No."[830]

If your answer is "Yes," please provide details and a citation to any case(s) or decision(s).

As stated, no agency responded "Yes" to the question.

15. If your answer is "Yes" to question 14(a) and/or 14(b), please state the basis of the claim(s) (*e.g.*, breach of contract, negligence, violation of a federal or state constitutional right to privacy, violation of a federal or state privacy and/or data-breach statute, and/or violation of a right to privacy at common law).

No agency answered "Yes" to questions 14(a) or 14(b).

16. In regard to questions 14 and 15, does your agency have sovereign immunity for any such claim or claims?

(please circle) YES NO

Five agencies responded "Yes" to the question.[831] Seventeen agencies responded "No."[832]

Transportation, and VIA Metropolitan Transit. Two agencies did not respond: Metropolitan Transportation Commission and Topeka Metropolitan Transit Authority.

[830] Berkshire Regional Transit Authority, Capital Area Transportation Authority, Capital District Transportation Authority, Central Florida Regional Transportation Authority, City of Madison Metro Transit,* Cobb Community Transit, Connecticut Department of Transportation, CT Transit,* Greater Cleveland Regional Transit Authority, Greater Hartford Transit District,* Greater Lynchburg Transit Company,* Laketran, Lane Transit District, Manchester Transit Authority, Metro Regional Transit Authority, Milwaukee County Transit System, Municipality of Anchorage, Public Transportation Department, OmniTrans, ORCA Regional Coordination Program, Port Authority of Allegheny County, Regional Transportation District, Salem-Keizer Transit, Space Coast Area Transit, Sunline Transit Agency, TriMet, and VIA Metropolitan Transit. The Metropolitan Transportation Commission, Topeka Metropolitan Transit Authority, and Westchester County Department of Public Works and Transportation did not respond to the question.

[831] Central Florida Regional Transportation Authority, Greater Cleveland Regional Transit Authority, Metro Regional Transit Authority, Port Authority of Allegheny County, and Regional Transportation District.

[832] Berkshire Regional Transit Authority, Capital Area Transportation Authority, Capital District Transportation Authority, Cobb Community Transit, CT Transit,* Greater Hartford Transit District,* Greater Lynchburg Transit Company,* Laketran, Lane Transit District, Manchester Transit Authority, Metra, Municipality of Anchorage, Public Transportation Department, Niagara Frontier Transportation Authority,* OmniTrans, ORCA Regional Coordination Program, Salem-Keizer Transit, and Sunline Transit Agency. The Metropolitan Transportation Authority, Metropolitan Transportation Commission, Milwaukee County Transit System, Space Coast Area

If your answer is "YES," please provide details.

The Central Florida Regional Transportation Authority reported that the agency is protected by Florida statute and that its liability is limited to $200,000 per person and $300,000 per event.

The Lane Transit District stated that the Oregon Tort Claims Act, Or. Rev. Stat. §§ 30.260 to 30.300, which is a limited waiver of sovereign immunity, may apply but the question requires "further input from the District's legal counsel."

Metro Regional Transportation Authority cited Ohio Revised Code, chapter 2744.

The Port Authority of Allegheny County stated that as a Commonwealth Agency it is subject to the protections afforded by sovereign immunity, 42 Pa. Con. Stat. Ann. § 8521, *et seq.*

The Regional Transportation District advised that "[t]o the extent such actions lie in tort or could lie in tort and RTD has not waived liability (*i.e.*, motor vehicles, dangerous buildings, etc.) for such actions, then RTD is immune from such claims actionable under state tort law related to breach of security of personal data and the right to privacy." See Colo. Rev. Stat. § 24-10-108.

Transit, Topeka Metropolitan Transit Authority, TriMet, Westchester County Department of Public Works and Transportation, and VIA Metropolitan Transit did not respond to the question or were unsure.

APPENDIX D

DOCUMENTS PROVIDED BY TRANSIT AGENCIES RESPONDING TO THE SURVEY

	Item No.
Central Florida Regional Transportation Authority d/b/a Lynx	
Participation Agreement between Bank of American, NA, Banc of America Merchant Services, LLC and Central Florida Regional Transportation Authority, dba LYNX	1
City of Raleigh, GoRaleigh, Raleigh, NC	
Information Technology Services Agreement	2
Gateway – Agency Funded Interchange Pass-through (IPT) Pricing	3
Metropolitan Transportation Authority, New York, NY	
The Metropolitan Transportation Authority and its Subsidiary and Affiliated Agencies' Internet Privacy Policy	4
ORCA Regional Coordination Program, Seattle, WN	
ORCA Privacy Statement	5
Port Authority of Allegheny County, Pittsburgh, PA	
Fare System Interoperability Agreement	6
PCI DSS Compliance	7
TriMet, Portland, OR	
Privacy Policy	8
Terms of Use	9
Privacy Statement, TriMet Mobile Ticketing Service Privacy Policy, August 12, 2013	10
Terms of Service, TriMet Mobile Ticketing Terms of Service, August 12, 2013	11
VIA Metropolitan Transit, San Antonio, TX	

ATTACHMENT D
PARTICIPATION AGREEMENT
BETWEEN

BANK OF AMERICA, N.A.
BANC OF AMERICA MERCHANT SERVICES, LLC
and
CENTRAL FLORIDA REGIONAL TRANSPORTATION AUTHORITY
dba LYNX

This Participation Agreement is entered into between Bank of America, N.A., Banc of America Merchant Services (together "Contractor") and Central Florida Regional Transportation Authority dba LYNX, ("Participant" as defined in the Scope of Work, Attachment A to the Master Contract with the Department of Financial Services). The Master Contract together with the Merchant Services terms and conditions and other attachments and incorporated documents are collectively referred to herein as the "Master Contract". Signatures on incorporated documents do not serve to negate the prevailing provisions of the Master Contract.

I. PARTICIPATION TERMS AND CONDITIONS

A. All defined terms in the Master Contract apply to this Participation Agreement.

B. By signing this Participation Agreement, the Participant and the Contractor agree to be bound by the terms of this Participation Agreement, and the Master Contract, in the performance of their obligations. By signing below, Participant represents that a copy of the Master Contract has been provided or made available to it.

C. If Participant is an Agency Participant, Participant hereby authorizes Contractor to share any and all information related to the Master Contract, excluding personally identifiable information of a cardholder, it has or obtains pursuant to this Participation Agreement and the Master Contract with representatives of the State of Florida and the specific Agency of the State of Florida to which it reports. If a Participant is a Local Government Participant, Participant hereby authorizes Contractor to share with the Department information that is required in the Dashboard under the Master Contract, excluding personally identifiable information of a cardholder.

D. The parties shall retain copies according to their retention schedules under applicable law.

E. Participants who elect specialized services that are subject to additional agreement terms offered as optional services under the Master Contract, are subject to those terms; however additional agreement terms do not serve to negate the prevailing provisions of the Master Contract.

II. MERCHANT SERVICES TERMS AND CONDITIONS

Participant will provide Contractor with updated business and financial information concerning Participant, including evidence of required licenses and other information and documents Contractor may reasonably request from time to time. All material marked Confidential that Contractor receives from Participant will be used only by Contractor, or Card Organizations or other third parties necessary to perform services under this Participation Agreement or related services and reporting. At any reasonable time, Contractor or any Card Organization may audit Participant's records relating to this Participation Agreement. Florida law, as applied to agreements made without reference to conflict of law provisions, governs the Master Contract and this Participation Agreement.

III. FEES TO BE PAID TO CONTRACTOR

A. The Participant agrees to pay the Contractor all fees and charges in Attachment B of the Master Contract.

B. Such fees and charges will be billed monthly to the Agency and Local Government Participants via an invoice process, unless a Local Government Participant elects to have the Contractor debit their Settlement Account.

IV. EFFECTIVE DATE AND TERMINATION

A. This Participation Agreement will become effective on the date it is signed by all parties.

B. Unless earlier terminated by one of the parties, this Participation Agreement remains in full force and effect until the earlier of (i) termination of the Master Contract or (ii) any date provided here: _____, not to exceed the expiration or termination of the Master Contract.

C. In the absence of a default by the other party, either party may terminate this Participation Agreement at any time by giving the other party ninety (90) days prior written notice. Either party may terminate this Participation Agreement after a default by the other party as provided in the Master Contract.

D. In the event of non-payment of fees because of insufficient funds in the Settlement Account or non-payment of an invoice for forty (40) days or more, Contractor may cease processing following 10 days' notice from Contractor according to the Master Contract. If Participant is an Agency Participant, payment shall be pursuant to section 215.422, F.S. If Participant is a Local Government Participant, payment shall be pursuant to legal requirements applicable to a Local Government Participant.

V. NOTICES

A. Any notice required or permitted to be given under this Participation Agreement or the Master Contract from one party to the other will be in writing and will be given and deemed to have been given when actually received, if hand delivered, delivered by telephonic facsimile transmission equipment and confirmed by telephone with and original mailed or hand-delivered thereafter or mailed by certified or registered mail with postage prepaid to the party or their successor at the address specified as follows:

1. Participant;
2. Contractor;
3. Routine notices given by Contractor to Participant, such as transaction details, changes in terms required by systems updates or Payment Card Organization changes and any reasonable notice required by the Contractor's services agreement or addenda, schedules, and attachments, may be delivered by electronic mail to the address provided by Participant above.

B. Either party may change the address to which notices are to be delivered by giving to the other party not less than ten (10) Business Days prior written notice thereof.

VI. ELECTION OF OPTIONAL SERVICES

Participant hereby elects to receive the following optional services pursuant to the terms and conditions contained in the various service addenda which are incorporated by reference in the Master Contract and attached thereto. The terms and conditions contained in a particular addenda shall not apply to Participant unless and until Participant elects, by indicating herein, or by future written election signed by the parties, to utilize such optional service.

☐ **Account Updater**

☐ Data File Manager

☐ **Dynamic Currency Conversion**

☐ **MobilePay**

☐ **PayPoint**

☐ **TransArmor**

VII. MISCELLANEOUS PROVISIONS

A. This Participation Agreement, incorporating the terms of the Master Contract, contains the entire understanding of the parties and supersedes any and all previous discussions, proposals, or agreements, if any, between the parties with respect to the subject matter hereof.

B. This Participation Agreement may not be amended except by an instrument in writing signed by an authorized representative of each of the parties.

C. Limitation of liability shall be according to PUR 1000-20 as modified in the Master Contract.

D. This Participation Agreement is binding on the parties and their successors and assigns.

Participant's Name: Central Florida Regional Transportation Authority dba LYNX

Select One: ☐ Agency Participant ☒ Local Government Participant

By: _____

Printed Name: John M. Lewis, Jr.

Title: Chief Executive Officer

Date: November 20, 2013

Contractor's Name: Bank of America, N.A.

By: _____

Printed Name: _____

Title: _____

Date: _____

Contractor's Name: Banc of America Merchant Services, LLC

By: _____

Printed Name: _____

Title: _____

Date: _____

INFORMATION TECHNOLOGY SERVICES AGREEMENT

This Information Technology Services Agreement (the "Agreement") is effective as of January 1, 2015 (the "Effective Date"), and is by and between the **CITY OF RALEIGH**, a North Carolina municipal corporation located at 222 West Hargett Street, Raleigh, North Carolina 27601 ("Client") and **LINK2GOV CORP.**, a Tennessee corporation located at 601 Riverside Avenue, Jacksonville, Florida 32204 (together with its subsidiaries and affiliates, "Link2Gov").

WITNESSETH:

WHEREAS, the City of Raleigh desires to procure a contractor to perform certain services; and

WHEREAS, the City of Raleigh has completed necessary steps for retention of professional and other services under applicable City of Raleigh policies; and

WHEREAS, the City of Raleigh has agreed to engage Link2Gov, and Link2Gov has agreed to contract with the City of Raleigh, for performance of services as described in this Agreement, and according to the further terms and conditions, set forth herein.

NOW THEREFORE, in consideration of sums to be paid to Link2Gov, and other good and valuable consideration, Link2Gov and the City of Raleigh do contract and agree as follows:

1. **General Terms and Addenda**. The Agreement consists of the attached General Terms and Conditions ("General Terms"), the Addenda listed below (each an "Addendum"), and any schedules, supplements, exhibits, and pricing attachments attached thereto:

   PAYDIRECT SERVICES ADDENDUM
   PRODUCTS AND SERVICES SCHEDULE (also referred to as the "Pricing Attachment")

2. **Commencement Date**. The Commencement Date of a Service already in use by Client as of the Effective Date shall be January 1, 2015. The Commencement Date of a Service not already in use by Client as of the Effective Date shall be as set forth in Section 2.1.1 of the General Terms.

3. **Term**. The Agreement shall remain in effect until the date on which Link2Gov is no longer obligated to provide any Service under any Addendum. Each Service, unless otherwise provided for in an Addendum or Supplement, shall have an initial term of thirty-six (36) months following the Commencement Date thereof (the "Initial Term"). Upon expiration of the Initial Term, the Service, including Software Maintenance Services if any, shall automatically be renewed for up to two (2) successive two (2)-year terms (each, a "Renewal Term") unless terminated by either party in writing at least one hundred eighty (180) days prior to the expiration of the Initial Term or of the then current Renewal Term.

4. **Non-Appropriation Clause**. The duration of the Initial Term shall not apply to this Agreement should Client fail to appropriate funds for any fiscal year. Client's fiscal year runs from July 1 through June 30. Client shall use all reasonable efforts to notify Link2Gov promptly upon adoption of the Client's annual budget by its legislative governing board if funding has not been approved for the next fiscal year. If this non-appropriation occurs, the Agreement shall be terminated except that Link2Gov shall be entitled to collect funds for all fiscal years for which funds have been appropriated and for all Services provided. Furthermore, Client shall either purchase or return any Equipment provided by Link2Gov in accordance with the provisions set forth in the Biller Solutions Services Addendum.

5. **Additional Service**. Additional Services may be added from time to time by amending this Agreement, including agreeing to additional Addenda, in accordance with the General Terms

SIGNATURES FOLLOW ON NEXT PAGE

IN WITNESS WHEREOF, the parties have caused their duly authorized officers or representatives to execute and deliver this Agreement as a legally binding obligation of such party.

CITY OF RALEIGH

Signature

Name (printed)
City Manager
Title

Date Signed

ATTEST

Signature

Name (printed)
(Deputy) Clerk-Treasurer
Title

Date Signed

THIS INSTRUMENT APPROVED AS TO FORM:

City Attorney

LINK2GOV CORP.

Signature

Name (printed)

Title

Date Signed

FIS

GENERAL TERMS AND CONDITIONS

1. **Introduction**. These general terms and conditions ("General Terms") together with each Addendum, now or hereafter agreed to by the parties are a part of the Information Technology Services Agreement (collectively, the "Agreement") between **CITY OF RALEIGH** of Raleigh, North Carolina ("Client") and **LINK2GOV CORP.** ("Link2Gov"). The pricing attachment(s) related to each Addendum are incorporated into and made a part of such Addendum. "Affiliate" means, with respect to a party, any entity which directly or indirectly, through one or more intermediaries, is controlled by, or is under common control with such party.

2. **Services**. If an Addendum describes the provision of services ("Services") by Link2Gov, the following subsections apply:

2.1 The "Commencement Date" of a Service not in effect as of the Effective Date is the earlier of: (i) the date the Services are first installed and available for Client's use in production; (ii) Client's first production use of the Services; or (iii) the commencement date agreed upon by the parties in writing. In the event that the parties are unable after a reasonable period of time to reach mutual agreement upon a Commencement Date, the Commencement Date shall be deemed to be the three (3)-month anniversary of the Effective Date. If commencement of a Service is delayed for more than ninety (90) days after the agreed upon Commencement Date and such delay is not due to Link2Gov's failure to meet its obligations hereunder, Link2Gov may suspend delivery of the Services and Client shall pay any one-time fees and minimum fees through the balance of the Initial Term. Upon the request of either party, the Commencement Date may be rescheduled to a new date that is mutually agreed upon in writing by both parties.

2.2 Each party shall dedicate sufficient resources, including the assignment of adequate personnel, to commence the Services as soon as practical following the Effective Date.

2.3 Link2Gov may postpone implementation of the Services if Client fails to timely provide required information or a circumstance arises that might jeopardize timely processing of transactions for other clients of Link2Gov.

3. **Responsibilities**.

3.1 Link2Gov Responsibilities.

3.1.2 If Client pays all applicable fees when due, Link2Gov shall provide (i) Client and Client's customers ("Customers") with access to and use of the Services in accordance with these General Terms, the applicable Addenda, and Link2Gov's then current standard user operating instructions and requirements made available to Client from time to time ("Specifications"), and (ii) Client with standard reporting, if any, associated with use of the Services. Link2Gov shall perform the Services in compliance with all Laws applicable to Link2Gov as a third party provider of that Service. "Law" means any law, rule, regulation, ordinance, code or order to which a party may be subject or under which a party may exercise rights.

3.1.3 Link2Gov shall perform an on-going review of federal Laws applicable to the provision of the Services and any software. Link2Gov shall maintain the features and functions for the Services and software in accordance with all federal Laws applicable to such features and functions, including new or amended federal Laws (as applicable and necessary to support compliance obligations), in a non-custom environment. In addition, Link2Gov shall work with Client in developing and implementing a suitable and commercially reasonable procedure or direction to enable Client to comply with state and local Laws applicable to the Services and software being provided to Client, and, to the extent commercially possible, modify the manner in which Link2Gov provides the Services prior to the regulatory deadline for such compliance. Any modification in the Services or software necessitated by such a change in state or local Laws shall be paid for by Client.

3.2 Client Responsibilities.

3.2.1 Client shall: (i) provide Customer information to Link2Gov in accordance with the Specifications; (ii) except to the extent due to Link2Gov's material breach of the Agreement, assume all risk and liability associated with transactions, including any risk of counterfeit, charged-back or fraudulent transactions; (iii) use the Services in accordance with the Specifications; (iv) timely deliver any Data (defined below) or other information necessary for the provision of the Services in an electronic form and format approved by Link2Gov; (v) be solely responsible for timely procuring any information or cooperation required from its Customers and suppliers or other third party(ies) in order to commence the Services; (vi) have sole responsibility for verifying the accuracy, completeness or authenticity of any Data furnished by Client or a third party; (vii) be solely responsible for training its employees and representatives to comply with all Laws applicable to Client and the procedures set forth in the Specifications or any manual or other literature provided to Client by Link2Gov; and (viii) comply with all Laws applicable to Client's business and its use of the Services,

including but not limited to those Laws relating to usury, truth-in-lending, fair credit reporting, equal credit opportunity, automated clearing house transfers, networks associations, electronic funds transfer, privacy and direct marketing, regardless of whether Client uses any forms or other Materials supplied by Link2Gov.

3.2.2 Client shall be responsible for monitoring and interpreting (and for complying with, to the extent such compliance requires no action by Link2Gov), the applicable Laws pertaining to Client's business ("Legal Requirements"). Based on Client's instructions, Link2Gov shall implement the processing parameter settings, features and options (collectively, the "Parameters") within Link2Gov's Services and systems that shall apply to Client, subject to the change request process in place between Link2Gov and Client to establish requirements, development arrangements and deployment timelines. Client shall be responsible for determining that such selections are consistent with the Legal Requirements and with the terms and conditions of any agreements between Client and its Customers. In making such determinations, Client may rely upon the written descriptions of such Parameters contained in the Specifications. Link2Gov shall perform the Services in accordance with the Parameters.

3.3 Data.

3.3.1 Client shall be solely responsible for the transmission of any information, data, records or documents (collectively, "Data") necessary for Link2Gov to perform the Services at Client's expense and shall bear any risk of loss resulting from that transmission until Link2Gov confirms receipt. Link2Gov shall bear the risk of loss resulting from Data transmitted to Client until Client confirms receipt. If Client directs Link2Gov to disclose Data to a third party, Client shall provide Link2Gov with written authorization to do so and bear any risk of loss or liability associated with that disclosure. In addition, Link2Gov shall have no liability for any claim resulting from the third party's use of that Data, and may, in its discretion, require the third party to enter into a written agreement with Link2Gov governing disclosure of that Data.

3.3.2 Link2Gov shall not be responsible for the accuracy, completeness or authenticity of any Data furnished by Client or a third party, and shall have no obligation to audit, check or verify that Data. If any Data submitted by Client or a third party to Link2Gov is incorrect, incomplete or not in the required format, Link2Gov may require Client to resubmit the Data or Link2Gov may correct the Data and bill Client its then-current rates for performing those corrections. Link2Gov shall attempt to notify Client prior to Client incurring such expense.

3.3.3 Client assumes all risk and expense associated with Data reconstruction for Data where Client's receipt has been confirmed by Link2Gov, except for those expenses incurred as a direct consequence of Link2Gov's breach of the Agreement. If Data reconstruction is ever required, the parties shall mutually agree on a schedule for that reconstruction.

3.4 Disaster Recovery. In accordance with FFIEC business continuity guidelines, Link2Gov has put in place a disaster recovery plan designed to minimize the risks associated with a disaster affecting Link2Gov's ability to provide the Services under the Agreement. Link2Gov's recovery time objective (RTO) under such plan is as set forth in the continuity program summary document made available to Client. Link2Gov will maintain adequate backup procedures in order to recover Client's Data to the point of the last available good backup, with a recovery point objective (RPO) as set forth in the continuity program summary document made available to Client. Link2Gov will test its disaster recovery plan annually. Upon request, Link2Gov will provide a summary of its disaster recovery plan and test results, excluding any proprietary information or NPI. Subject to the confidentiality provisions of Section 10 of this Agreement, Client authorizes Link2Gov to provide Client's Data to external suppliers in order to test and prepare for disaster recovery, as well as provide replacement services in the event of a disaster. Client acknowledges and agrees that Link2Gov is not responsible for and does not assume any liability for Client's failure to adopt a disaster recovery program for Client's facilities. Further, Link2Gov has no liability to Client for securing business interruption insurance or other insurance for Client's protection.

3.5 Changes to Services. Link2Gov may change any features, functions, brand, third party provider, attributes of the Services, or any element of its systems or processes, from time to time, provided that such changes do not have a material adverse impact on the performance or cost of the Services. Client shall not rely on identification of specific brands associated with or names of third party providers of a service as an obligation of Link2Gov to use any particular brand or third party provider. If Client requests a change to the Services, the parties shall negotiate the terms for such change, which terms will be set forth in a mutually agreed upon statement of work ("SOW").

3.6 Transition Assistance. Upon termination of the Agreement or an Addendum, Link2Gov shall cooperate in the transition of the Services to Client or a replacement service provider and, if requested by Client, perform ancillary services for additional fees. However, no master files, transaction data, test data, record layouts or other similar information shall be provided by Link2Gov until: (i) Client and, if applicable, the replacement service provider, have executed Link2Gov's deconversion confidentiality agreement, the terms of which shall be reasonable to all parties; (ii) Client has fully paid all outstanding amounts; (iii) Client has completely prepaid Link2Gov's fees for deconversion assistance; and (iv) the parties

mutually agree on a date for deconversion that is at least one hundred eighty (180) days following Link2Gov's receipt of Client's notice of deconversion. If the one hundred eighty (180)-day period ends between the third week of November and the third week of January, the time period for completing deconversion may be extended until the first week of February. In addition, upon termination of the Agreement, Link2Gov may, at Client's request and expense, continue to provide the corresponding Services(s) until the deconversion is completed, provided the parties agree to such continuation in writing.

3.7 Problem Reporting and Resolution. Client shall timely report any problems encountered with the Services. Link2Gov shall provide a toll-free telephone number for problem reporting. Link2Gov shall promptly respond to each reported problem based on its severity, the impact on Client's operations and the effect on the Services. Link2Gov shall use reasonable commercial efforts to either resolve each problem or provide Client with information to enable Client's personnel to resolve it.

4. **Services**. The Services to be delivered to Client shall be as set forth in the PayDirect Services Addendum and any attachments, exhibits, or supplements thereto.

5. **Use of Services**. Except as otherwise permitted in the Agreement or in writing by Link2Gov, Client agrees to use the Services only for its own internal business purposes to service its U.S.-based accounts for its Customers and will not sell or otherwise provide, directly or indirectly, any of the Services or any portion thereof to any third party. Client agrees that Link2Gov may use all suggestions for improvement and comments regarding the Services that are furnished by Client to Link2Gov in connection with the Agreement, without accounting or reservation. Except as otherwise may be set forth herein or in writing between the parties, Client shall be responsible for handling all Customer inquiries relating to the Services.

6. **Materials**. As a convenience, Link2Gov may provide Client with sample forms, procedures, scripts, marketing materials or other similar information (collectively, "Materials"). Client shall have a license to use Materials, if any, solely in connection with its use of the Services during the Initial Term and any Renewal Term and solely in a manner that is consistent with the Specifications. Client's right to use the Materials shall expire immediately upon termination of the Agreement, or a particular Addendum. Client is responsible for its use of Materials and bears sole liability for any such use.

7. **Training**. Except as may be otherwise agreed in writing, Link2Gov will provide its standard initial train-the-trainer training regarding the use and operation of the Services to Client by web-based training or in person at an Link2Gov training location (in which case, travel would be at Client's expense) at Link2Gov's then-current rates and on a mutually-agreed date and time. Following such initial training, Client is responsible for its trainer(s) training Client's employees on the use and operation of the Services. Additional training may be provided by Link2Gov upon Client's request, including onsite training at Client's location, as mutually agreed to by the parties regarding topics, duration and fees and expenses.

8. **Fees and Other Charges**.

8.1 Client shall pay all fees and charges set forth in the pricing attachment(s). Recurring fees, if any, shall be paid beginning on the Commencement Date; provided, however, that notwithstanding anything to the contrary contained in Section 20.5 below, for any Services in use by Client as of the Effective Date, Client shall continue to pay such recurring fees applicable to such Services under Client's prior agreement with Link2Gov up to the Commencement Date.

8.2 Link2Gov may increase any pass-through fees (including, without limitation, interchange fees, processor fees, courier, and telecommunications expenses) outside of its control as its cost for such items increases. These adjustments will be effective for each product or Service on the first day of the calendar month of each anniversary of the Effective Date of the Addendum or agreement that relates to the product or service. Fees, costs and expenses owed by Client are exclusive of charges for materials, work, hardware, software or travel not otherwise detailed in the Agreement, a SOW, or pricing attachment.

8.3 Travel time, if required, will be charged at Link2Gov's standard hourly rates, but will not exceed eight (8) hours per day per resource.

8.4 The parties acknowledge that the proposed scope of work contemplates agency-funded pricing as of the Effective Date. If convenience fee pricing is incorporated into the services provided by Link2Gov under this Agreement, Link2Gov reserves the right to review and adjust all convenience fee pricing on a semi-annual basis in June and December. This adjustment may be consistent with the then most recent ECI adjustment or three percent (3%) whichever is greater. Items that will be considered in the review of convenience fees may include, but are not limited to: regulatory changes, card association rate adjustments, card association category changes, bank/processor dues and assessments, average consumer payment amounts, and card type utilization.

8.5 For any amount that is not paid within sixty (60) days after its due date, Client shall pay a late fee equal to the lesser of one and one-half percent (1½%) per month of the unpaid amount or the maximum interest rate allowed by Law.

8.6 In the event of over-billing, Link2Gov will correct the error by credit to Client. If Client was under-billed, Link2Gov will add the under-billed amount to a future invoice. Any under-billed amounts will be invoiced on an invoice separate from the regular invoices submitted to Client for the Services. Link2Gov may utilize any amounts owed to Client under the Agreement to pay or reimburse Link2Gov for amounts owed by Client.

8.7 All charges and fees to be paid by Client under the Agreement are exclusive of any applicable withholding, sales, use, excise, value added or other taxes. Any such taxes for which Link2Gov is legally or contractually responsible to collect from Client shall be billed by Link2Gov and paid by Client. Client agrees to reimburse Link2Gov for any taxes, penalties and interest assessed by any taxing authority arising out of the Agreement. Link2Gov shall pay and hold Client harmless for any taxes on Link2Gov property, income or payroll. Client agrees to hold Link2Gov harmless for any sales, use, excise, value added or other taxes assessed by a taxing authority arising out of the Agreement. In the event of any assessment by a taxing authority, both parties agree to cooperate with each other to resolve issues in order to minimize such assessment.

8.8 Link2Gov shall submit invoices to accountspayable@raleighnc.gov or City of Raleigh, Accounts Payable, PO Box 590, Raleigh North Carolina 27602-0590. Invoices shall be submitted on a monthly basis and undisputed amounts shall be due from Client within thirty (30) days of receipt of invoice by Client.

9. **Intellectual Property**.

9.1 Client shall not directly or indirectly decompile, reverse compile, reverse engineer, reverse assemble or otherwise derive a source code equivalent for any software that may be provided to Client. Client is not acquiring a copyright, patent or other intellectual property right in any Service, software, Deliverable, Specifications or Materials, or in any data, modifications, customizations, enhancements, changes or work product related thereto. "Deliverable" means any work product or other item (whether tangible or intangible) created by Link2Gov or provided by Link2Gov to Client pursuant to the Services, or software, and which may be described more particularly in an Addendum, SOW, or other document signed by the parties.

9.2 Any intellectual property rights that existed prior to the Effective Date shall belong solely to the party owning them at that time. Neither party shall be entitled to any copyright, trademark, trade name, trade secret or patent of the other party.

9.3 Client shall not alter, obscure or revise any proprietary, restrictive, trademark or copyright notice included with, affixed to, or displayed in, on or by the Services, software, or Specifications.

10. **Confidentiality**.

10.1 Each party shall treat information received from the other that is designated as "confidential" at or prior to disclosure ("Confidential Information") as strictly confidential. Link2Gov designates the Services, software, any Deliverables, Specifications and the terms of the Agreement, and all information related to the foregoing, as its Confidential Information, subject to the public records laws of the State of North Carolina. Client designates Customer information qualifies as "Non-public Personal Information" under the Gramm-Leach-Bliley Act of 1999 or its state law equivalents ("NPI") as its Confidential Information. Any information disclosed verbally by Link2Gov that is confidential will be designated as such when it is disclosed.

10.2 Each party shall: (i) restrict disclosure of the other party's Confidential Information to employees, agents and Affiliates solely on a "need to know" basis in accordance with the Agreement; provided, however, that Link2Gov may use, disclose, and archive Data including, without limitation, Client's Confidential Information, provided that Link2Gov shall first aggregate all such Data and remove any NPI prior to any disclosure to third parties not bound by the confidentiality provisions of the Agreement; (ii) advise its employees and agents that have access to the Confidential Information of their confidentiality obligations; (iii) require agents to protect and restrict the use of the other party's Confidential Information; (iv) use the same degree of care to protect the other party's Confidential Information as it uses to safeguard its own Confidential Information of similar importance, but in no event less than a reasonable degree of care; (v) establish procedural, physical and electronic safeguards, designed to meet the objectives of the FFIEC Interagency Guidelines, to prevent the compromise or unauthorized disclosure of Confidential Information. Client shall notify Link2Gov of any breach of Link2Gov's Confidential Information as soon as possible following determination of such breach. Link2Gov shall notify Client of any breach of NPI as soon as possible following determination of such breach and shall comply with all federal and state Laws regarding NPI that are applicable to it as a third party processor.

10.3 Confidential Information shall remain the property of the party from or through whom it was provided. Except

for NPI, neither party shall be obligated to preserve the confidentiality of any information that: (i) was previously known; (ii) is a matter of public knowledge; (iii) was or is independently developed; (iv) is released for disclosure with written consent; or (v) is received from a third party to whom it was disclosed without restriction. Disclosure of Confidential Information shall be permitted if it is: (a) required by Law; (b) in connection with the tax treatment or tax structure of the Agreement; or (c) in response to a valid order of a U.S. court or other governmental body, provided the owner receives written notice (which may be via electronic mail) and is afforded a reasonable opportunity to obtain a protective order. Upon termination of the Agreement, each party shall, to the extent permitted by law, destroy the other party's Confidential Information relating to the Agreement in a manner designed to preserve its confidentiality, or, at the other party's written request and expense, return it to the disclosing party. Upon termination of the Agreement, each party shall destroy any remaining Confidential Information of the other party in the same manner or, if so requested, return it to the disclosing party at its expense.

10.4 Notwithstanding any other provision of the Agreement, the Agreement and all material submitted to Client by Link2Gov (or its agents or affiliates) (including, but not limited to, any proposal materials) are subject to the public records laws of the State of North Carolina, which are contained in Chapter 132 of the North Carolina Statutes Annotated, and it is the responsibility of Link2Gov to properly designate materials that may be protected from disclosure as trade secrets under North Carolina law as such and in the form required by law prior to the submission of such materials to Client. Link2Gov understands and agrees that Client may take any and all actions necessary to comply with federal, state and local laws and/or judicial orders and such actions will not constitute a breach of the terms of the Agreement. To the extent that any other provision of the Agreement conflicts with this section, the provisions of this section shall control.

11. **Indemnification.**

11.1 Link2Gov shall defend Client and its officers, employees, directors, agents and shareholders, in their individual capacities or otherwise, from and against any and all Claims (as defined in this Section 11.1) asserted by a third party (other than an Affiliate of Client) against Client, and shall indemnify and hold harmless Client from and against any damages, costs, and expenses of such third party awarded against Client by a final court judgment or an agreement settling such Claims in accordance with this Section 11.1. As used in this Section 11.1, the term "Claim" means any action, litigation, or claim by a third party alleging (i) personal injury or property damage caused by Link2Gov's gross negligence or willful misconduct in connection with this Agreement; (ii) Link2Gov's failure to comply with all federal laws, rules and regulations applicable to Link2Gov as a provider of a Service; or (iii) that a Service, Software, or Deliverable infringes an effective U.S. Patent or a registered trademark or copyright; provided, however, that Link2Gov shall not be liable for any infringement or alleged infringement that results, in whole or in part, from: (a) use of a Service, Software or Deliverable in a manner or for a purpose not specifically described in the Agreement (including the Addenda) or Specifications; (b) use of a Service, Software or Deliverable in combination with computer programs, processes, hardware, software, data, systems, or services owned, licensed or provided by someone other than Link2Gov; (c) Client's products or services; (d) modification, change, amendment, customization, or adaptation of any Service, Software, or Deliverable not made wholly by Link2Gov; or (e) Client's failure to implement corrections or changes provided by Link2Gov. If a claim of infringement has been asserted, or in Link2Gov's opinion is about or likely to be asserted, Link2Gov may, at its option either: (1) procure for Client the right to continue using the Service, Software or Deliverable; (2) replace or modify the Service, Software, or Deliverable so that it becomes non-infringing; (3) terminate the applicable Addendum or SOW and refund all pre-paid fees covering future use of the Service, Software or Deliverable; or (4) defend the action on Client's behalf and pay any associated costs or damages.

11.2 The obligation to indemnify under this Section 11 is contingent upon: (i) the indemnified party's promptly notifying the indemnifying party in writing of any Claim subject to such indemnity obligation; (ii) the indemnifying party's having sole control over the defense and settlement of the Claim; (iii) the indemnified party's reasonably cooperating during defense and settlement efforts; (iv) the Claim(s) not arising, in whole or in part, out of the action or inaction of the indemnified party; and (v) the indemnified party's not making any admission, concession, consent judgment, default judgment or settlement of the Claim or any part thereof.

12. **Limitation of Liability, Disclaimer of Warranties, and Certain Losses.**

12.1 Limitation of Liability. LINK2GOV'S TOTAL LIABILITY FOR A SERVICE IS LIMITED IN ALL CASES AND IN THE AGGREGATE TO $250,000 PER CLAIM. NOTWITHSTANDING THE FOREGOING, NEITHER PARTY SHALL BE LIABLE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, DELAY OR PUNITIVE DAMAGES WHATSOEVER (INCLUDING BUT NOT LIMITED TO, DAMAGES FOR LOSS OF BUSINESS PROFITS OR REVENUE, BUSINESS INTERRUPTION, LOSS OF INFORMATION, OR OTHER PECUNIARY LOSS), EVEN IF SUCH PARTY WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

12.2 Disclaimer of Liability for Certain Losses. Notwithstanding anything to the contrary contained in Section 12.1 above, under no circumstances shall Link2Gov be liable for any losses, claims, demands, penalties, actions, causes of

action, suits, obligations, liabilities, damages, delays, costs or expenses, including reasonable attorney's fees (collectively, "Losses") caused, directly or indirectly, in whole or in part, by: (i) Client; (ii) a third party under the control of Client, other than Link2Gov's authorized agents; (iii) use of attachments, features, or devices not authorized by the Specifications; (iv) improper or inadequate conditions at a non-Link2Gov site; (v) improper or incomplete installation not caused by Link2Gov or its authorized agents; (vi) equipment changes, reconfigurations, upgrades or relocations performed by one other than Link2Gov or its authorized agents; (vii) abuse, misuse, alteration or use that is inconsistent with the terms of the Agreement or Specifications; (viii) incorrect or incomplete Data supplied by Client or its agents; (ix) software, hardware or systems not supplied by Link2Gov; (x) a Force Majeure Event; or (xi) a failure that is not directly attributable to Link2Gov or under Link2Gov's direct control. In the event of any error by Link2Gov in processing any Data or preparing any report or file hereunder, Link2Gov's sole obligation shall be to correct the error by reprocessing the affected Data or preparing and issuing a new file or report at no additional cost to Client; provided, however, Link2Gov's obligation herein is contingent upon Client notifying Link2Gov of the error within thirty (30) business days of Client discovering the error or two (2) processing cycles (whichever period is later) after Client receives the improperly processed Data, report or file.

12.3 Disclaimer of Warranties. **EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT, LINK2GOV DISCLAIMS ANY AND ALL OTHER WARRANTIES, CONDITIONS, OR REPRESENTATIONS (EXPRESS OR IMPLIED, ORAL OR WRITTEN) WITH RESPECT TO THE SERVICES, SOFTWARE, EQUIPMENT, AND MATERIALS PROVIDED UNDER THIS AGREEMENT, INCLUDING, WITHOUT LIMITATION, ANY AND ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS OR SUITABILITY FOR ANY PARTICULAR PURPOSE, OR ERROR FREE OPERATION (EVEN IF CREATED BY THE INTERNATIONAL SALE OF GOODS CONVENTION, AND WHETHER OR NOT LINK2GOV KNOWS, HAS REASON TO KNOW, HAS BEEN ADVISED, OR IS OTHERWISE IN FACT AWARE OF ANY SUCH PURPOSE), WHETHER ALLEGED TO ARISE BY LAW, BY REASON OF CUSTOM OR USAGE IN THE TRADE, OR BY COURSE OF DEALING. IN ADDITION, Link2Gov DISCLAIMS ANY WARRANTY OR REPRESENTATION TO ANY PERSON OTHER THAN CLIENT WITH RESPECT TO THE SERVICES, SOFTWARE, EQUIPMENT, AND MATERIALS PROVIDED UNDER THIS AGREEMENT.**

13. **Outsourcing Management; TSP Audit and Vendor Diligence Information**.

13.1 Outsourcing and TSP Diligence Generally. Link2Gov will cooperate with Client to meet its responsibilities to diligence and audit Link2Gov as its third party technology service provider (TSP), as contemplated by the FFIEC IT Examination Handbook and related guidelines (TSP Guidelines). Link2Gov will regularly make available audit reports and materials that address Client's vendor management and diligence requirements under the TSP Guidelines. Specific information regarding the available materials meeting the TSP Guidelines is available under the "Vendor Diligence and Audit Materials" on the Link2Gov Client Portal.

13.2 Vendor Diligence and Audit Materials. Through its Link2Gov Client Portal and Link2Gov Governance Site, Client will have continuous electronic access to audit reports, attestations, and other detailed information regarding Link2Gov's internal systems testing and procedures, and Link2Gov's information security and data privacy controls. These audit materials and attestation evidence Link2Gov's compliance with all industry and regulatory standards and include recent independent audits (such as SSAE 16's), third party attestations and certifications (such as AT101's and PCI AOC's), and detailed information and testing results regarding physical, technical and administrative controls utilized by the Service business lines within Link2Gov and the security of Client's Confidential Information.

13.3 Information Security and Risk Management In-Depth Conferences. Client may attend any or all of the Link2Gov In-Depth Conferences, which provide detailed audit information and in-depth in-person discussions with Link2Gov's senior executive team regarding Link2Gov's information security and risk management processes and system testing results. The In-Depth Conferences provide Client with comprehensive vendor diligence information, including (i) a thorough, interactive review of Link2Gov enterprise-wide security and system controls, and (ii) specific assessments of industry standards and best practices for financial technology information security and risk management. Currently, Link2Gov offers four (4) In-Depth Conferences each year, with clients attending a two-day event onsite at different Link2Gov facilities.

13.4 Governmental Access. Link2Gov shall permit governmental agencies that regulate Client in connection with a Service performed by Link2Gov to examine Link2Gov's books and records to the same extent as if that Service was being performed by Client on its own premises, subject to Link2Gov's confidentiality and security policies and procedures.

14. **Notices**. Except as otherwise specified in the Agreement, all notices, requests, approvals, consents and other communications required or permitted under the Agreement shall be in writing and shall be personally delivered or sent by (i) first class U.S. mail, registered or certified, return receipt requested, postage pre-paid; or (ii) U.S. express mail, or other, similar overnight courier service to the address specified below. Notices shall be deemed given on the day actually received by the party to whom the notice is addressed.

FIS

In the case of Client:
City of Raleigh
222 West Hargett Street
Raleigh, North Carolina 27601
Attn.: Treasury Office
Copy to: City Manager
Copy to: City Attorney

In the case of Link2Gov:
Fidelity Information Services, LLC
601 Riverside Avenue
Jacksonville, Florida 32204
Attn: Strategic Account Manager
Copy to: General Counsel

15. **Use of Names and Trademarks**. Neither party shall use the other party's logos, trademarks or stock exchange ticker symbol unless pre-approved in writing.

16. **Relationship**. Link2Gov is an independent contractor. Neither Link2Gov nor any of its representatives are an employee, partner or joint venturer of Client. Link2Gov has the sole obligation to supervise, manage and direct the performance of its obligations under the Agreement. Link2Gov reserves the right to determine who will be assigned to perform its obligations, and to make replacements or reassignments as it deems appropriate. Each party shall be solely responsible for payment of compensation to its respective personnel, and assumes full responsibility for payment of all federal, state, local and foreign taxes or contributions imposed or required under unemployment insurance, social security and income tax laws with respect to such personnel. Except as expressly stated in the Agreement, neither party shall be an agent of the other, nor have any authority to represent the other in any matter. To the extent that Link2Gov engages a subcontractor, Link2Gov shall remain solely responsible for the performance of the subcontracted work. Client shall have no recourse, and shall assert no claim, against any subcontractor of Link2Gov.

17. **Insurance**. Link2Gov agrees to maintain, on a primary basis and at is sole expense, at all times during the life of the Agreement the following coverages and limits. The requirements contained herein, as well as Client's review or acceptance of insurance maintained by Link2Gov is not intended to and shall not in any manner limit or qualify the liabilities or obligations assumed by Link2Gov under the Agreement.

Commercial General Liability – Combined single limit of no less than $1,000,000 each occurrence and $2,000,000 aggregate. Coverage shall not contain any endorsement(s) excluding nor limiting Product/Completed Operations, Contractual Liability or Cross Liability.

Automobile Liability – Limits of no less than $1,000,000 Combined Single Limit. Coverage shall include liability for Owned, Non-Owned and Hired automobiles. In the event Link2Gov does not own automobiles, Link2Gov agrees to maintain coverage for Hired and Non-Owned Auto Liability, which may be satisfied by way of endorsement to the Commercial General Liability policy or separate Auto Liability policy. Automobile coverage is only necessary if vehicles are used in the provision of services under the Agreement and/or are brought on a Client site.

Worker's Compensation & Employers Liability – Link2Gov agrees to maintain Worker's Compensation Insurance in accordance with North Carolina General Statute Chapter 97 with statutory limits and employees liability of no less than $1,000,000 each accident.

Additional Insured – Link2Gov agrees to endorse Client as an Additional insured on the Commercial General Liability, Auto Liability and Umbrella Liability if being used to meet the standard of the General Liability and Automobile Liability. The Additional Insured shall read **'City of Raleigh is named additional insured as their interest may appear'.**

Certificate of Insurance – Link2Gov agrees to provide Client a Certificate of Insurance evidencing that all coverages, limits and endorsements required herein are maintained and in full force and effect, and Link2Gov shall provide a minimum thirty (30) day endeavor to notify, when available, by Link2Gov's insurer. If Link2Gov receives a non-renewal or cancellation notice from an insurance carrier affording coverage required herein, or receives notice that coverage no longer complies with the insurance requirements herein, Link2Gov agrees to notify Client within five (5) business days with a copy of the non-renewal or cancellation notice, or written specifics as to which coverage is no longer in compliance. **The Certificate Holder address should read:**

City of Raleigh
Post Office Box 590
Raleigh, NC 27602-0590

Umbrella or Excess Liability – Link2Gov may satisfy the minimum liability limits required above under an Umbrella or Excess Liability policy. There is no minimum Per Occurrence limit of liability under the Umbrella or Excess Liability, however, the Annual Aggregate limits shall not be less than the highest 'Each Occurrence' limit for required policies. Link2Gov agrees to endorse City of Raleigh as an 'Additional Insured' on the Umbrella or Excess Liability, unless the Certificate of Insurance states the Umbrella or Excess Liability provides coverage on a 'Follow-Form' basis.

Professional Liability – Including **Cyber Liability** – Limits of no less than $1,000,000 each occurrence and $2,000,000 aggregate.

All insurance companies must be authorized to do business in North Carolina.

18. **Termination and Additional Remedies**.

18.1 Termination. In addition to any other remedies, either party may terminate the Agreement on thirty (30) days advance written notice if the other party: (i) fails to cure a material breach within thirty (30) days of receiving written notice to do so; (ii) is the subject of a dissolution, reorganization, insolvency or bankruptcy action that is not dismissed within forty-five (45) days of being filed; (iii) suffers the appointment of a receiver, conservator or trustee; (iv) commits any act related to the Services with the intent to defraud the other party; or (v) discontinues performance under the Agreement because of a binding order of a court or regulatory body. Either party may also terminate the Services on thirty (30) days' advance written notice if the other party fails to cure a material breach related to such Services within thirty (30) days of receiving written notice to do so. If a breach cannot reasonably be cured within thirty (30) days, the non-breaching party may not terminate the Services so long as the breaching party promptly commences work and completes correction within ninety (90) days of receiving written notice of the breach. Notwithstanding the foregoing, Link2Gov may terminate the Agreement if Client (a) fails to maintain required balances in the Settlement Account associated with a Service (if any is required), and fails to remedy that deficiency within forty-eight (48) hours of Link2Gov requesting it to do so, (b) cure any material violation of applicable Law within thirty (30) days of Link2Gov requesting it to do so, or (c) sells, transfers or assigns all or substantially all of its Services-related accounts to a third party that does not agree in writing with Link2Gov to be bound by the terms of the Agreement.

18.2 In addition to the termination rights set forth above, Link2Gov may terminate a Service, in whole or in part, without penalty, if Link2Gov's agreement to use any third-party software or service upon which the Service relies expires or is terminated; provided, however, that prior to any such termination, Link2Gov shall use commercially reasonable efforts to either (i) extend the applicable expiration or termination date so that its provision of the Service hereunder is not interrupted; (ii) procure a third-party software or service similar to the expired or terminated software or service in order to continue to deliver the Service without interruption and without reduction in quality or increase in cost to Client; or (iii) develop another workaround that allows Client to continue to receive the Service without interruption and without reduction in quality or increase in cost.

18.3 This section is omitted intentionally.

18.4 Early Termination. Either party may terminate this Agreement by giving the other party one hundred eighty (180) days' prior written notice, which notice shall specify the effective date of the termination.

18.5 Due to the likelihood of irreparable injury, each party shall be entitled to seek an injunction against the other for any breach of confidentiality, indemnification and intellectual property obligations.

19. **Export Restrictions and Unlawful Activity**.

19.1 Link2Gov's Confidential Information is subject to export controls under applicable federal and state Laws, rules and regulations. Accordingly, Client shall: (i) remain in compliance with all requirements associated with such Laws; (ii) cooperate fully with any audit related to such Laws; and (iii) not utilize Link2Gov's Confidential Information in any country that is embargoed by the U.S. government. Client shall be solely responsible for the importation of Link2Gov's Confidential Information, including obtaining any approval or permit necessary for importation or use.

19.2 Neither Client nor any of its directors, officers, agents, employees or other persons associated with or acting on its behalf: (i) have received or will receive any unlawful contribution, gift, entertainment or other payment from Link2Gov; (ii) is a governmental entity; or (iii) is in violation of, or will violate any applicable anti-corruption or anti-bribery laws, rules or regulations. Link2Gov shall have an irrevocable right to immediately terminate the Agreement or any other relationship with Client if this subsection is breached.

20. **Data Security**. Link2Gov represents and warrants that it maintains security standards sufficient to meet Payment Card Industry (PCI) compliance standards and that it will undergo annual recertification by certified Quality Security Assessors. Link2Gov will promptly notify Client if, at any point, if it is determined to not be PCI compliant. Link2Gov is responsible for securing data once it is contained within the Link2Gov network. Link2Gov will provide assistance to Client where it is permissible under PCI rules and regulations. Link2Gov is not responsible for PCI compliance when the data is outside the Link2Gov network and outside of permissible PCI compliance rules and regulations.

21. **Miscellaneous**.

21.1 Neither party shall assign, subrogate or transfer any interest, obligation or right arising out of the Agreement without prior written consent from the other party, which shall not be unreasonably withheld; provided however, that Link2Gov may freely assign this Agreement (i) in connection with a merger, corporate reorganization or sale of all or substantially all of its assets, stock or securities, or (ii) to any entity which is a successor to the assets to the business of Link2Gov without prior written consent from Client. Notwithstanding the foregoing, if Client determines it is in violation of a federal, state, or local law or a binding resolution as a result of Link2Gov's assignment of this Agreement, Client may terminate this Agreement up on written notice to Link2Gov.

21.2 The Agreement shall be governed by the laws of the state of North Carolina, without regard to internal principles relating to conflict of laws. In the event of litigation to enforce the terms of the Agreement, the parties consent to venue in an exclusive jurisdiction of the courts of Wake County, North Carolina, and the Federal District Court for the Eastern District of North Carolina.

21.3 Link2Gov shall not be liable for any loss, damage or failure due to causes beyond its reasonable control, including strikes, riots, earthquakes, epidemics, terrorist actions, wars, fires, floods, weather, power failure, telecommunications outage, acts of God or other failures, interruptions or errors not directly caused by Link2Gov ("Force Majeure Event").

21.4 Each party represents and warrants that it has full legal power and authority to enter into and perform its obligations without any additional consent or approval.

21.5 The Agreement (including these General Terms, all Addenda and the pricing attachment(s)) together with any attachments thereto, constitute the entire agreement and understanding of the parties with respect to its subject matter. All prior agreements, understandings and representations regarding the same or similar services are superseded in their entirety. In the event of a conflict, ambiguity or contradiction in documents, the documents will take precedence over each other in accordance with the following ranking: (i) Addenda; (ii) exhibits and attachments; (iii) Specifications; and (v) these General Terms. The Agreement may only be modified by a written document signed by both parties. The parties do not intend, nor shall there be, any third party beneficiary rights.

21.6 No waiver of any provisions of the Agreement and no consent to any default under the Agreement shall be effective unless in writing and signed by the party against whom such waiver or consent is claimed. No course of dealing or failure to strictly enforce any provision of the Agreement shall be construed as a waiver of such provision for any party's rights. Waiver by a party of any default by the other party shall not be deemed a waiver of any other default.

21.7 If any provision(s) of the Agreement, including any Addenda, supplements, attachments and exhibits hereto, is determined to be invalid, illegal, void, or unenforceable by reason of any Law, rule or regulation, administrative order, judicial decision, or public policy, such provision(s) shall not affect any other provision of the Agreement, and the Agreement shall be interpreted and construed as if the invalid, illegal, void, or unenforceable provision had not been included to the extent necessary to bring the Agreement within the requirements of such Law, rule or regulation, administrative order, judicial decision, or public policy. In addition, in such event, the parties agree to negotiate in good faith to modify the Agreement to carry out the parties' original intent as closely as possible and to the extent lawful. This Agreement shall not be construed more strongly against either party, regardless of who is more responsible for its preparation. The headings that appear in the Agreement are inserted for convenience only and do not limit or extend its scope.

21.8 Termination of the Agreement shall not impact any right or obligation arising prior to termination, and in any event, Sections 10, 11, 12, 13, 21.2, 21.8 of the Agreement shall survive termination of the Agreement.

21.9 In consideration of the signing of the Agreement, the parties hereto for themselves, and their agents, officials, employees, and servants agree not to discriminate in any manner on the basis of race, color, creed, national origin, gender, age, handicap, or sexual orientation with reference to the subject matter of the Agreement, no matter how remote. The parties further agree in all respects to comply with the provisions of the City of Raleigh Ordinance 1969-889, as amended. This section is incorporated into the Agreement for the benefit of Client and its residents and may be enforced by action for specific performance, injunctive relief, or other remedy as provided by law. This provision shall be binding on the successors and assigns of the parties with reference to the subject matter of the Agreement.

FIS

PAYDIRECT SERVICES ADDENDUM

1. **Introduction**. Link2Gov shall provide to **CITY OF RALEIGH** of Raleigh, North Carolina ("Client") the biller solutions services as indicated below (each a "Service" and, collectively, the "Services") pursuant to this PayDirect Services Addendum to the Agreement. In addition to the terms and conditions set forth in the General Terms and the signature page accompanying this Addendum, the following terms shall apply with respect to the Services.

2. **Services**. Link2Gov shall provide one or more of the following: online, point-of-sale, and/or telephonic payment processing Services using Link2Gov's systems ("System") as described in this Addendum for Client's credit card, debit card, electronic benefits transfer and/or electronic Check transactions ("Transactions"). Link2Gov will provide the Services to Client either directly or through one or more of its affiliated companies or subcontractors, in accordance with the corresponding Specifications. References to Link2Gov in this Addendum include such entities.

2.1 Payment Processing. Link2Gov shall transmit Transaction files for authorization and settlement through Link2Gov's certified payment processor(s) (an "Approved Processor"). Funds for Transactions processed by Link2Gov hereunder shall be submitted to Client's designated bank account as follows: no more than two (2) business banking days after all Transactions that are successfully processed prior to Client's end of day cut time (e.g., a Transaction authorized at 2:00 p.m. ET on Monday will be submitted on Wednesday). Link2Gov makes no representation or warranty as to when funds will be made available by Client's bank.

2.2 Support. Link2Gov shall provide Client with support (Client Support), twenty-four (24) hours per day, seven (7) days per week, subject to commercially reasonable downtime, with toll-free voice communications lines, or email, and representatives to address service requests. Link2Gov will also provide support for end users (Customer Support) via a toll-free number.

2.3 Electronic Check Authorization. If Client has elected to accept electronic Checks as a form of payment, the following subsections apply. For the purposes of this Addendum, "checks" means checks drawn on accounts held in the U.S. ("Check(s)").

2.3.1 As part of the implementation plan, Client shall select risk management controls governing Check acceptance and assumes sole responsibility for its choice of controls.

2.3.2 Link2Gov shall provide confirmation on a submitted ABA number as part of the Service to assist Client with its decision whether to accept a Check and shall route Checks accepted by Client.

2.3.3 Client hereby authorizes Link2Gov to debit the Client's financial institution account in the amount of any returned item that is received by Link2Gov.

2.4 Implementation/Professional Services. Link2Gov shall perform the professional services for Client as set forth in the Pricing Attachment and the implementation plan and shall perform additional professional services as mutually agreed upon by the parties from time to time under this Addendum, provided that either party may require execution of a separate mutually acceptable professional services agreement prior to Link2Gov's performance of professional services other than those set forth in the Pricing Attachment or the implementation plan.

2.5 User Interface. For the "User Interface", Link2Gov shall provide a user interface to the Services in the form of a Virtual Terminal, a telephony based payment system developed by Link2Gov or its designee through which a User (as defined below) may perform a Transaction ("IVR System"), or Internet Private Label Site (the "UI Services").

2.5.1 Domain Names; Client Brand Features.

2.5.1.1 Unless otherwise agreed by Link2Gov and Client, Link2Gov shall own all of the unique addresses that identify the location of a website(s) on the Internet ("Domain Name(s)") used to provide the UI Services, provided that Client shall own any and all Domain Names used for the Internet Private Label Site or Private Label Virtual Terminal. For purposes of this Addendum:

a. "Internet Private Label Site" means a secure payment website on the Internet that presents the Look and Feel of Client's existing website, and is developed, hosted and maintained by Link2Gov pursuant to this Addendum, and at which a User may perform a Transaction;

b. "Look and Feel" means the elements of graphics, design, organization, presentation, layout, user interface, navigation and stylistic convention (including the digital implementations thereof) which are provided by, and unique to, Client;

c. "User" means any person or entity who processes, or for whom Client processes, a Transaction using the UI Services;

d. "Virtual Terminal" means a secure payment site on the Internet that is developed, hosted and maintained by Link2Gov pursuant to this Addendum, at which Client may process Transactions made by Users; and

e. "Private Label Virtual Terminal" is a Virtual Terminal that presents the Look and Feel of Client and may include certain of the Client Brand Features, defined below.

2.5.1.2 Link2Gov has the right to reject and remove any information made available to Users via the UI Services, which may include, without limitation, text, graphics, data and other similar materials ("Content") and/or trademarks, service marks, Look and Feel, logos and other distinctive brand features of Client supplied to Link2Gov by Client ("Client Brand Features") at any time if Link2Gov reasonably believes that any such materials infringe any third party Intellectual Property Rights, are libelous or invade the privacy or violate other rights of any person, violate applicable Laws or regulations, jeopardize the health or safety of any person, or are otherwise detrimental to the goodwill of Link2Gov.

2.5.1.3 Link2Gov shall correct or cause to be corrected, with reasonable promptness and at its own cost, any errors in the UI Services that are caused by Link2Gov's failure to perform according to the terms of this Addendum or the Agreement. In no event shall Link2Gov be liable for any costs of corrections in excess of its own costs incurred to correct an error that Link2Gov is solely responsible for correcting.

2.5.1.4 Ownership.

a. All Client Brand Features shall be owned exclusively by Client. To the extent Link2Gov possesses any ownership rights in the Client Brand Features, Link2Gov hereby irrevocably assigns to Client all right, title and interest in and to all such Client Brand Features, which includes, without limitation, all of Client's Intellectual Property Rights therein. For purposes of this Addendum, "Intellectual Property Rights" means any and all now known or hereafter known tangible and intangible: (i) rights associated with works of authorship throughout the world, including, without limitation, copyrights, moral rights, and mask-works; (ii) trademark and trade name rights and similar rights; (iv) trade secret rights; (v) patents, designs, algorithms and other industrial property rights; (vi) other intellectual property rights, whether arising by operation of law, contract, license, or otherwise; and (vii) registrations, initial applications, renewals, extensions, continuations, divisions or reissues thereof now or hereafter in force (including any rights in any of the foregoing). If Link2Gov has any such rights that cannot be assigned to Client, Link2Gov waives the enforcement of such rights, and if Link2Gov has any rights that cannot be assigned or waived, Link2Gov hereby grants to Client an exclusive, irrevocable, perpetual, worldwide, fully paid license to such rights (which includes the right to sublicense). Client represents and warrants that it owns the Client Brand Features and all Intellectual Property Rights therein and that such Client Brand Features do not infringe upon any other material or violate or infringe upon the Intellectual Property Rights of any other party.

b. Subject only to Section 2.5.1.4.a. above, all Intellectual Property Rights directly or indirectly related to the UI Services (which may include certain software provided by Link2Gov) shall be owned exclusively by Link2Gov (collectively, the "Link2Gov Property"). To the extent Client possesses any ownership rights in the Link2Gov Property, Client hereby irrevocably assigns to Link2Gov all right, title and interest in and to all such Link2Gov Property, which includes, without limitation, all applicable Intellectual Property Rights thereto. If Client has any such rights that cannot be assigned to Link2Gov, Client waives the enforcement of such rights, and if Client has any rights that cannot be assigned or waived, Client hereby grants to Link2Gov an exclusive, irrevocable, perpetual, worldwide, fully paid license to such rights (which includes the right to sublicense).

c. Client hereby grants Link2Gov a non-exclusive, worldwide license to use the Client Brand Features for Link2Gov to perform its obligations hereunder. The scope of the foregoing license shall be limited as specified herein, and shall not include any right to use, copy, modify, publish, license, sublicense, sell, market or distribute such Client Brand Features, unless expressly authorized herein. Client is not hereby granted any right or license to use any trademarks, trade names, or service marks of Link2Gov or its affiliates and subsidiaries.

3. **Convenience Fee**. If Client elects to charge a convenience fee to Customers, the amount of such fee(s) shall be specified in the implementation plan. Client authorizes Link2Gov to collect each convenience fee.

4. **Transaction Errors**. Link2Gov's sole responsibility for any Transaction error or reversed Transaction is to determine whether any mechanical, procedural, or processing problems occurred at Link2Gov during the preparation of the Transaction file (including but not limited to rejection of files) and, if necessary, reprocess and resubmit the Transaction file without additional charge. In the event that a Transaction is reversed or refunded to any Customer of Client, for any

reason, Link2Gov may offset such amount against funds remitted to Client, or invoice Client for such amount. Client shall pay any such invoice in accordance with the General Terms and this Addendum. In such instance, Link2Gov shall notify Client of the Customer's name and account number.

5. **Client Warranties**.

5.1 As a condition to its receipt of the Services, Client represents and warrants that Client shall execute and deliver any and all applications, agreements, certifications or other documents required by Networks or other third parties whose consent or approval is necessary for the processing of Transactions. "Network" is an entity or association that operates, under a common service mark, a system which permits participants to authorize, route, and settle transactions among themselves, including, for example, networks operated by VISA USA and MasterCard, Inc., NYCE Corporation, American Express, and Discover.

5.2 Client represents, warrants and agrees that it does and will comply with applicable Laws and regulations and Network rules, regulations or operating guidelines. Client shall notify Link2Gov in writing as soon as possible in the event a claim is either threatened or filed against Client by any governmental organization having jurisdiction over Client related to the processing Services. Client shall also notify Link2Gov in writing as soon as possible in the event a claim is either threatened or filed against Client relating to Transactions or the Services or a fine or other penalty is assessed or threatened against Client relating to Transactions or the Services.

5.3 Client represents, warrants and agrees that it is and will continue to be in full compliance with all applicable requirements of the Client Information Security Program of VISA, the Site Data Protection Program of MasterCard, and similar programs of other Networks, and any modifications to such programs that may occur from time to time. Upon the request of Link2Gov, Client shall provide Link2Gov with documentation reasonably satisfactory to Link2Gov verifying compliance with this Section.

5.4 Client hereby grants Link2Gov the full right, power and authority to request, receive and review any data or records reflected in a Transaction report. Client represents and warrants that it has the full right and authority to grant the rights set forth in the preceding sentence.

6. **Reserved**.

7. **Additional Service Terms**. Link2Gov agrees that the following additional service terms shall apply to the PayDirect Services provided to Client.

7.1 Link2Gov shall transfer credit card funds directly to an official depository bank located in North Carolina as designated by Client. Allowable expenses and monthly service fees shall not be subtracted from the gross amounts deposited.

7.2 Client elects to compensate Link2Gov through a direct monthly fee and not as deductions to revenues received, i.e., "Direct Pay".

7.3 Should Client develop a need for additional merchant accounts or services during the Initial Term, Link2Gov shall provide applicable services under the same conditions as apply to accounts that exist at the time additional merchant accounts or services are added.

7.4 Client determines its daily cut-off times and all transactions are batched accordingly. As of the Effective Date, Client's cut-off time is nightly at midnight.

7.5 Each merchant ID requested as part of the implementation process is identified by Link2Gov with a unique Merchant Code and Settlement Code. Each Settlement Code can be associated with the same or different Client demand deposit account to settle to. A separate settlement deposit will be submitted per merchant account.

7.6 As of the Effective Date, Saturday and Sunday activity will be separated at Client's request.

7.7 Link2Gov's responsibility relating to PCI compliance is set forth in Section 20 of the General Terms.

Gateway - Agency Funded Interchange Pass-through (IPT) Pricing

Link2Gov will provide Client with transaction processing (merchant) services for all applications under an Agency Funded Interchange Pass-through pricing model. Link2Gov reserves the right to not accept any payment type in situations where doing so may be in violation of the rules and regulations governing that payment type.

Merchant Services	Rate	Frequency
All Debit and Credit Cards[1]	Pass-through[2]	Per Transaction
ACH/eCheck Processing	$0.12	Per Transaction
Transaction Based Rate	$0.18	Per Transaction

Ancillary Services	Rate	Frequency
Reporting and Statement Fee	Waived	Per Application Per Month
ACH and eCheck Returns	$3.00	Per Event
Chargebacks and Adjustments	$10.00	Per Event
Voice Authorizations	Waived	Per Event
24 hr Settlement Fee (wire)	$40.00	Per Settlement
48 hr Settlement (ACH)	Waived	Per Settlement

Examples - Client would absorb the following amounts for a $50.00 transaction:

- Paying with Visa and MasterCard, Discover, or AMEX = IPT + Link2Gov charges ($0.18 Transaction Fee) = Unknown Amount
- Paying via eCheck: For a transaction of any size the convenience fee would be $.12/per eCheck.

[1] Credit, Checkcard, PINless and Signature Debit included.

[2] Pass-through includes all Interchange Qualifications rates (per volume and per item fees), dues, acquirer fees, and assessments. These rates may vary by card type, transactions, and over time, and rates are subject to change solely at the determination of the association or issuer.

Additional Product and Services Pricing

Implementation Services	Rate	Frequency
New Application Setup (Standard)	$500.00	Per Application at Setup
API Development	$2,500 + Resource Rate	Per Application
WEB Development (Non-Standard)	$2,000 + Resource Rate	Per Application
IVR Development	$4,500 + Resource Rate	Per Application
Resource Rate	$150.00	Per Hour
Hosting and Maintenance	$150.00	Per Application Per Month
Application Training – Remote	TBD	Per event
Application Training – Onsite	$2,500 + Costs	Per event
IVR Line Fee[3]	$0.10	Per Minute
Opt Out for CSR Assistance[4]	$1.50	Per Minute

[3] IVR Based, All Payment Types included, Credit, Debit, ACH, successful or unsuccessful transactions.

[4] Opt out for Customer Service Representative (CSR) assistance. Should consumer need assistance in making a payment via the IVR application in an Agency Absorbed model the Agency will be billed $1.50/minute. Please note the CSR will not make the payment on behalf of the consumer but only walk them through the payment process.

Metropolitan Transportation Authority, New York, NY

The Metropolitan Transportation Authority and its Subsidiary and Affiliated Agencies' Internet Privacy Policy 4

APPENDICES

The Metropolitan Transportation Authority and its Subsidiary and Affiliated Agencies' Internet Privacy Policy

Overview

The Metropolitan Transportation Authority and its subsidiary and affiliated agencies, MTA Metro-North Railroad, MTA Long Island Rail Road, MTA New York City Transit, MTA Bridges and Tunnels, and MTA Capital Construction (collectively the "MTA Agencies") are committed to protecting your privacy when you use the MTA website (the "MTA Website"). Consistent with the provisions of the New York State Internet Security and Privacy Act, the New York State Freedom of Information Law, and the New York State Personal Privacy Protection Law, this Policy describes the MTA Agencies' privacy practices regarding information collected from users of the MTA Website.

This Policy describes what information is collected when you access the MTA Website and how that information is used. Because this Policy only applies to the MTA Website itself and not linked websites, you should examine the privacy policy of any other websites that you access from the MTA Website.

Please carefully read this Policy before submitting any personal information, including your e-mail address, for notification of service updates, initiating an online transaction, providing information with respect to employment opportunities, or for any other reason. Please note that this Policy may change from time to time without special notice to you, so please check back to review the most recent version of this Policy.

For purposes of this Policy, "personal information" means any information concerning a natural person, which, because of a name, number, symbol, mark, or other identifier, can be used to identify that natural person. The MTA Agencies only collect personal information about you when you provide that information voluntarily by sending an e-mail, initiating an online transaction, or submitting information for employment purposes. The information that is available to us from your visit to an MTA Website depends upon which sections of the website you visit and what actions you take during such visit.

Information Collected Automatically When You Visit the MTA Website

The MTA Agencies monitor MTA Website user traffic and patterns, and automatically collect certain non-personal information about your visit such as the internet domain name from which you access the MTA Website, the type of browser and operating system you used, the date and time of your visit, the pages you visit, and the referring web site address, if any. This information is used to improve the content of the MTA Website and to help the MTA Agencies understand how users are interacting with the MTA Website. This information is not collected for commercial marketing purposes and the MTA Agencies will not sell or otherwise disclose the information collected from the MTA Website for commercial marketing purposes.

Cookies and Web Beacons

The MTA Agencies may use cookies to track how you visit certain pages on the MTA Website. The use of cookies is a standard practice among Internet websites. Cookies are small amounts of data that are sent to your browser from our web servers and are stored on your computer's hard drive, not on our site. Cookies collect information that includes the server your computer is logged into and your browser type. Cookies used in connection with the MTA Website do not retrieve any other data from your hard drive, or

capture your e-mail address or any other personal information. Accepting cookies is required if you want to use certain of the MTA Website functions because they are essential for site administration and security.

From time to time, MTA also may use web beacons, alone or in conjunction with cookies, to determine what MTA ads your browser is shown, what ads you click and other actions you take on the Internet, to help us better provide relevant products, services and information to you and to help us effectively measure advertising effectiveness. We also collect information on our website through the use of web beacons or 1x1 pixels. A web beacon is a transparent 1x1 pixel image that has been placed on a web page and sends a signal when a user has visited that page. A web beacon does not contain any personal information. No information that is personally identifiable to you is transmitted to the third party using the web beacon. The third party is required to protect the privacy of the information it receives using Web beacons or cookies and is not allowed to use the information it receives for any purpose beyond what is necessary to assist us. We do not sell, rent, trade, or otherwise distribute information about you gathered through the web beacons or pixels with any third parties.

Information Collected When You E-mail the MTA Website, Initiate an Online Transaction, or Submit Information For Employment Purposes

During your visit to the MTA Website you may place an order for goods or services, submit an inquiry, and/or submit information concerning opportunities for employment. The information, including personal information, volunteered by you in initiating such transactions is used by one or more of the MTA Agencies to provide you with goods, services, and information or to undertake the employment review process. The information collected by one or more of the MTA Agencies may be shared among them and disclosed by them for those purposes that may be reasonably ascertained from the nature and terms of the transaction in connection with which the information was submitted. The information is not collected for commercial marketing purposes and the MTA Agencies will not sell or otherwise disclose the information collected from the MTA Website for commercial marketing purposes.

The MTA Agencies do not collect any personal information about you during your visit to the MTA Website unless you provide that information voluntarily by sending an e-mail or initiating an online transaction such as filling out a registration or completing an order form, or for purposes of employment. You may choose not to send us an e-mail, register online for a service, complete an online order form, or submit information for employment purposes. While your choice not to participate in these activities may limit your ability to receive specific services or products through the MTA Website, it will not prevent you from requesting services or products from the MTA Agencies by other means and will normally not have an impact on your ability to take advantage of other features of the MTA Website, including browsing or downloading most publicly available information.

The MTA Agencies do not knowingly collect personal information from children or create profiles of children through the MTA Website. Users are cautioned, however, that the collection of personal information submitted in an e-mail or through an online transaction will be treated as though it was submitted by an adult, and may, unless exempted by federal or state law, be subject to public access. The MTA Agencies strongly encourage parents and teachers to be involved in children's Internet activities and to provide guidance whenever children are requested or otherwise have the opportunity to provide personal information online.

Disclosure of Information Collected Through The MTA Website

The collection of information through the MTA Website and the disclosure of that information are subject to the provisions of the New York State Internet Security and Privacy Act. The MTA Agencies will only collect personal information through the MTA Website or disclose personal information collected through

the MTA Website if the user has consented to the collection or disclosure of such personal information or under the circumstances described below. The voluntary disclosure of personal information to the MTA Agencies by the user, including participation in an online transaction, whether solicited or unsolicited, constitutes consent to the collection and disclosure of the information by the MTA Agencies for the purposes reasonably ascertainable from the nature and terms of the disclosure.

However, the MTA Agencies may collect or disclose personal information without user consent if the collection or disclosure is: (1) necessary to perform the statutory duties of the MTA Agencies, or necessary for the MTA Agencies to operate a program authorized by law, or authorized by state or federal statute or regulation; (2) made pursuant to a court order or required by law; (3) required for the purpose of validating the identity of the user; or (4) of information to be used solely for statistical purposes that is in a form that cannot be used to identify any particular person.

Further, the disclosure of information, including personal information, collected through the MTA Website is subject to the provisions of the New York State Freedom of Information Law and the New York State Personal Privacy Protection Law.

The MTA Agencies may disclose personal information to federal or state or local law enforcement authorities to enforce the MTA Agencies' rights against unauthorized access or attempted unauthorized access to the MTA Agencies' information technology assets or against other inappropriate use of the MTA Website or other MTA property.

Retention of Information Collected Through the MTA Website

The information collected through the MTA Website is retained by the MTA Agencies in accordance with the applicable records retention and disposition requirements of New York law. Information concerning these records retention and disposition schedules may be obtained athttp://www.archives.nysed.gov/a/records/mr_pub_mi1_part1.shtml and by contacting the MTA Website's Privacy Compliance Officer listed below.

Access to and Correction of Personal Information Collected Through the MTA Website

Any user may submit a request to the MTA Website's Privacy Compliance Officer to determine whether personal information pertaining to that user has been collected and retained through the MTA Website. Any such request shall be made in writing to the address below and must be accompanied by reasonable proof of identity of the user. Reasonable proof of identity may include verification of a signature, inclusion of an identifier generally known only to the user, or other appropriate identification. Such a request should be mailed to the MTA Website Privacy Compliance Officer:

MTA Website Privacy Compliance Officer
Metropolitan Transportation Authority
347 Madison Avenue
New York, New York 10017

The MTA Website Privacy Compliance Officer shall, within (5) business days of the date of the receipt of a proper request: (i) provide access to the personal information; (ii) deny access in writing, explaining the reasons therefor; or (iii) acknowledge the receipt of the request in writing, stating the approximate date when the request will be granted or denied, which date shall not be more than thirty (30) days from the date of the acknowledgment.

In the event that the MTA Agencies have collected and retained personal information pertaining to a user through the MTA Website and that information is to be provided to the user pursuant to the user's request, the MTA Agencies shall inform the user of his or her right to request that the personal information be amended or corrected under the procedures set forth in section 95 of the New York Public Officers Law.

Confidentiality and Integrity of Personal Information Collected Through the MTA Website

The MTA Agencies are strongly committed to protecting personal information collected through the MTA Website against unauthorized access, use, or disclosure. Consequently, the MTA Agencies limit employee access to personal information collected through the MTA Website to only those employees who need access to the information in the performance of their official duties. Employees who have access to this information are required to maintain its confidentiality and disclose it only as permitted under this Policy.

In addition, the MTA Agencies have implemented procedures to safeguard the integrity of their information technology assets, including, but not limited to, authenticating, monitoring, auditing, and encrypting. Security procedures have been integrated into the design, implementation, and day-to-day operations of the MTA Website as part of our continuing commitment to the security of electronic content as well as the electronic transmission of information.

As an additional security measure, many areas of the MTA Website require the use of a User ID and Password to help protect your confidential information. This allows the MTA Agencies to verify who you are, thereby allowing you access to your account information, and preventing unauthorized access. You are responsible for maintaining the confidentiality of your password and account, and agree to immediately notify the MTA Agencies of any unauthorized use of your password or account or any other breach of security.

For website security purposes and to maintain the availability of the MTA Website for all users, the MTA Agencies employ software to monitor traffic to identify unauthorized attempts to upload or change information or otherwise damage the MTA Website.

One or more of the MTA Agencies have retained independent contractors or third party service providers to perform special contract functions in connection with the MTA Website, including, but not limited to, providing e-commerce services, computer programming, storing and managing customer information, processing transactions, and providing advice about and support of our products and services. As users navigate the MTA Website they may not be able to identify which services are provided by such contractors or providers and which services are provided directly by the MTA Agencies. These third party contractors or service providers may obtain and store and/or process your personal information on their own computer systems. The contracts between the MTA Agencies and these entities require them to treat your personal information securely.

Links

In order to provide users with certain information, the MTA Agencies provide links to the websites of local, State, and federal government agencies, and to the websites of other public and private organizations. A link does not constitute an endorsement of the content, viewpoint, accuracy, opinions, policies, products, services, or accessibility of that website. Once you link from the MTA Website to another website you are subject to the terms and conditions of that website, including, but not limited to, its Internet privacy policy, if any.

Disclaimer

The information provided in this Policy should not be construed as giving business, legal, or other advice, or warranting as fail proof, the security of information provided through the MTA Website.

Contact Information

For questions regarding this Policy, please *contact the MTA Website Privacy Compliance Officer via email*

or by mail to:

MTA Website Privacy Compliance Officer
Metropolitan Transportation Authority
2 Broadway, Room C4.64
New York, New York 10004

Enterprise
Electronic Informati

Release of
Electronic Custome

ORCA Privacy Statement

Last revised August 10, 2015

Welcome to ORCA, which offers people the opportunity to use a single card to ride buses, trains, streetcars and ferries throughout the Puget Sound region.

The ORCA Privacy Statement explains how information is collected and treated by the Agencies when an individual chooses to participate in the ORCA Program. This includes summarizing the type of data residing on an ORCA Card, as well as the type of data that is stored centrally. You'll learn the differences between a card that has been registered so the value can be replaced if lost, an unregistered card, and a card that has been distributed to an individual by an employer or other institution.

ORCA Privacy at a Glance
Before getting into the full ORCA Privacy Statement that is below, this section provides brief answers to a few of the most frequent questions about ORCA data. You should refer to the full statement below for more in-depth information.

What information can my employer access regarding my use of an employer-provided ORCA Card?
If an ORCA Card is given to you by an employer or other institution, that "Business Account" entity retains ownership of the card and can obtain access to data about transactions involving the card. Transaction data includes the date, time of day, fare and bus route, ferry or train station where a card was used. The ORCA system collects this data specific to the card serial number.

What electronic information can be "read" from an ORCA card?
An ORCA Card's microchip contains electronic information that does NOT include names but could include data in such fields as the type of card, Business Account ID number (if issued to an employer or other institution), the passenger type expiration date or date of birth (if present), fare products loaded onto the card including E-purse value and passes, the history of the prior ten (10) trip transactions (time, date, route and fare when the card was used) and the history of the prior five (5) revalue transactions (See Sec. 8.2). In order to keep the processing time to several milliseconds when an ORCA Card is tapped, the information on the card is generally not encrypted. However, date of birth or passenger type expiration date, if present, is encrypted.

The electronic information on the card can be read by ORCA reader devices. Anyone with physical possession of a card, whether or not he or she is the rightful owner, can use the card until it is empty or blocked, as well as read some of the electronic data at an ORCA service location. It is also possible that an ORCA Card's unencrypted data could be electronically "read" by a non-ORCA device if the card uses the same frequency and were to come within the range of the reader device. However, the unencrypted data which is not in plain text would require interpretation.

1.0 Application of this Privacy Statement

1.1 ORCA stands for One Regional Card for All. The ORCA Program allows you to use a single fare card when taking the public transportation services provided by the participating Agencies.

1.2 This Privacy Statement explains how information is collected and treated by the Agencies when an individual participates in the ORCA Program. With the exceptions noted below, this Privacy Statement applies to the products and services provided by the Agencies under the ORCA Program, including but not limited to ORCA Cards, ORCA Products, ORCA Websites and ORCA Customer Services.

1.3 ORCA Websites and any ORCA Customer Services that require Personal Identifying Information (PII) are not intended for minors. We will not accept or request information from individuals we know to be under 18.

1.4 This Privacy Statement does not apply to the following information, including PII you provide to a Retailer. If you provide PII to a Retailer (e.g. your name and credit card number), such PII is not covered by this Statement. The Retailer, not the Agencies, is responsible for the collection, storage, transmittal, safekeeping and use of that information.

1.5 This Privacy Statement does not apply to information, including PII you provide to your employer, school or other Business Account to which the Agencies sell Business Cards and ORCA Products. If you provide PII to your employer, school or other Business Account in connection with obtaining a Business Card or ORCA Product, such PII is not covered by this Statement. The Business Account, not the Agencies, is responsible for the collection, storage, transmittal, safekeeping or use of that information.

2.0 Definitions

As used in this Privacy Statement, the following terms shall have the meanings indicated.

2.1 "Agency(ies)" means one or more of the following public transportation providers and the contractors and subcontractors which these Agencies, individually or collectively, have retained for purposes related to the ORCA Program.

a. Central Puget Sound Regional Transit Authority ("Sound Transit");
b. City of Everett ("Everett Transit");
c. King County ("King County Metro");
d. Kitsap County Public Transportation Benefit Area ("Kitsap Transit");
e. Pierce County Public Transportation Benefit Area ("Pierce Transit");
f. Snohomish County Public Transportation Benefit Area ("Community Transit"); and
g. The State of Washington acting through the Washington State Department of Transportation,
h. Washington State Ferries Division ("WSF")

For clarification, the term "Agency(ies)" does not include Business Accounts or Retailers.

2.2 "Autoload" is the Cardholder-authorized process for automatically loading ORCA Products on a registered ORCA Card and making a corresponding charge against the Cardholder's credit card to pay for the loaded product.

2.3 "Business Account" means an entity other than an individual customer, including but not limited to an employer, educational institution or social service agency, that purchases Business Cards and products for distribution to its employees, students or other program participants according to the terms of an agreement with one of the Agencies.

2.4 "Business Card" is a type of ORCA Card issued to a Business Account for distribution to individuals who are eligible participants in the Business Account's transportation program.

2.5 "Card Verification Number (CVN)" is the three-digit number printed on the card at manufacture, which

is required for security purposes to register an ORCA Card online and other card-not-present functions.

2.6 "Low Income" is a type of ORCA Card issued to individuals who are eligible for reduced fare in King and Kitsap counties based on income. Low income ORCA cards are not transferable.

2.7 "ORCA" is the trademark acronym for One Regional Card for All.

2.8 "ORCA Card" is the smart card that can be presented for fare payment on train, bus and ferry services provided by, and in accordance with the terms established by the Agencies. ORCA Card can mean cards issued to individuals and Business Cards, unless the context indicates it means one or the other.

2.9 "ORCA Customer Services" are the facilities and services of one or more of the Agencies that exchange information with customers regarding the ORCA Program and sell ORCA Cards and ORCA Products, including customer service counters, telephone call-in centers, mail-in centers, business account support and ticket vending machines.

2.10 "ORCA Product(s)" or "Product(s)" are any transit fare payment option offered for sale within the ORCA Program including, but not limited to, monthly or period passes and E-purse.

2.11 "ORCA Program" means the equipment, systems, facilities, ORCA Cards, ORCA Products, ORCA Websites, data, information, and any products and services related to the regional fare coordination and payment program implemented by the Agencies using smart cards as the common media for fare payment on their public transportation services.

2.12 "ORCA Websites" are the following public-facing websites: www.orcacard.com and www.orcacard.biz.

2.13 "Personally Identifying Information" (PII) means the following information when collected by the Agencies under the ORCA Program: a natural person's name; and, if combined with said name, the address, telephone number, e-mail address, date of birth, Regional Reduced Fare Permit-related information (as defined below), photo, and check/debit card/credit card information.

2.14 "Retailer" or "ORCA Retailer" is a retail business or other entity that, under an agreement with an Agency, is equipped with a device for customers to add ORCA products on an ORCA Card or to purchase a new adult ORCA Card.

2.15 "Regional Reduced Fare Permit (RRFP)" is a type of ORCA Card issued to individuals who are eligible for reduced fares by one of the Agencies based on the individual's disability or age (65 and older). RRFP ORCA cards are not transferable. A valid Medicare card is proof of eligibility for an RRFP.

2.16 "Youth" is a type of ORCA Card issued to individuals who are eligible for reduced fare based on the individual's age (6 to 18 years old). Youth ORCA cards are not transferable.

3.0 Customer Services Requiring Information

3.1 No information is required if you pay cash fares for your public transportation rides. Information may be needed, however, if you choose to use services such as an ORCA Card or an ORCA Website. If you contact ORCA Customer Services by mail, telephone, e-mail or in-person, that contact may be logged and the information you provide may be collected by the ORCA Program. The type of information required will vary with the services sought. If you decline to submit information for some services, the Agencies may be unable to provide you those services. You may still use cash to purchase ORCA Cards or ORCA Products as described in Section 3.3.

3.2 Your PII is collected in the ORCA Program when you:

a. Use a check, debit card or credit card to purchase an ORCA Card or ORCA Product or authorize "Autoload" of ORCA Products to load on an ORCA Card.

b. Establish your eligibility for youth fare, the Regional Reduced Fare Permit for seniors and persons with disabilities, King County Access paratransit program or King County and Kitsap County Low Income fare programs.
c. Purchase an ORCA Card or Product that requires proof of eligibility under a reduced fare program (e.g. a youth fare, a Regional Reduced Fare Permit, a Low Income fare, or a King County Access pass product).
d. Register an ORCA Card to take advantage of the replacement card benefit or other registration benefits.
e. Surrender your registered card and request a refund of the remaining E-purse value.
f. Request customer services such as an e-mail reply or phone call from an ORCA representative.
g. Use the functionality on password-protected areas of ORCA Websites.

3.3 You may obtain an ORCA Card and purchase ORCA Products without providing PII if you use cash (or money order) and do not register your ORCA Card. You may also anonymously visit many pages on the ORCA Websites. We ask for PII only to the extent needed to provide you with customer services. If you are uncomfortable providing the requested information, or with the use of that information, you may simply decline to receive that level of service or participate in that particular program. For example, to avoid purchasing an ORCA Product by credit card online, you may simply pay cash at an ORCA Customer Services location.

3.4 ORCA Websites and any ORCA customer services that require PII are not intended for minors. We will not accept or request PII from individuals we know to be under 18.

4.0 Information Related to ORCA Card Issuance and Optional Registration

4.1 When an ORCA Card is first issued, issuance information is created both in the ORCA central system and in the card's electronic memory. This issuance information includes: the card's serial number; the type of card; for a Youth card, the qualifying date of birth to enable automatic conversion to Adult card upon the expiration of youth status upon end of qualifying age; for an RRFP (Regional Reduced Fare Permit,) an expiration date for temporary disabilities and any eligibility for a personal care attendant; for a senior RRFP card, the qualifying date of birth; for an ORCA Business Card, the identifying number of the Business Account.

4.2 An ORCA Card that is also a Regional Reduced Fare Permit may have a photo, name or other PII printed on its face. That type of information might also be on ORCA Cards that are used as identification badges distributed by employers or other Business Accounts.

4.3 When you provide PII to establish your eligibility for reduced fare programs, certain PII is retained in the ORCA Program to enable the Agencies to administer and monitor use of these reduced fare programs.

a. When eligibility for youth fares is established, the date of birth (or for Business Cards, the date that the cardholder is no longer eligible for a youth fare) is retained in the ORCA Program.
b. When eligibility for a Regional Reduced Fare Permit is established, the following is retained in the ORCA Program: first name, last name, middle initial (if applicable), date of birth (for senior and youth only), whether or not a personal care attendant is eligible, address and expiration date (if applicable).
c. When eligibility for King County's Access paratransit program is established, the following information is retained in the ORCA Program to enable loading Access Products on an ORCA Card: first name, last name, middle name (if applicable), date of birth, address, Access ID and Access eligibility expiration date.

d. When eligibility for Low Income fare is established, the expiration date is retained in the ORCA Program.

4.4 An individual is not required to register an ORCA Card with the Agencies unless the individual requests an RRFP or to purchase a pass for use on King County's Access paratransit service. If an individual chooses to provide PII to the Agencies for purposes of registering an ORCA Card, such PII is held by the ORCA Program and associated with the card serial number.

5.0 Information Related to the Purchase of ORCA Cards and ORCA Products

5.1 When you purchase an ORCA Card or an ORCA Product, the system collects varying amounts of information depending on your method of payment. You will need to provide PII if your purchase is by check, credit card or debit card (see Section 6 below). Regardless of how you pay, the system will collect the following information when you purchase an ORCA Card or an ORCA Product.

a. Date and time of the purchase.
b. The serial number of the ORCA Card and the number of the device used to load an ORCA Product if the ORCA Card is presented at a Retail Revalue Site, an Agency customer service office or a ticket vending machine.
c. The serial number of the subject ORCA Card and the processing location information about the purchase if the card is not presented for loading the ORCA Product at the time of purchase (e.g. online purchase; mail or telephone order; or Autoload).
d. The amount/type of ORCA Product purchased.
e. The amount paid and method of payment (e.g. cash, check, credit or debit card) and related-information as listed in Section 6.

5.2 Information about the purchase of ORCA Cards and ORCA Products is associated with the card's serial number. If you have provided PII (e.g. to establish eligibility for a reduce fare program or to make a purchase using a check, credit card or debit card), the PII that is retained can be associated with the card serial number.

5.3 The ORCA Card contains the current amount/type of ORCA Products available for use. It can also contain certain information related to the last five (5) purchases of ORCA Products, including the date and time the product was loaded on the card, the amount/type of ORCA Product loaded, the payment method and the payment amount.

6.0 Information Related to Purchases Using Credit Cards, Debit Cards and Checks

6.1 If you purchase an ORCA Card or ORCA Product by a means other than cash payment (or money order), you must provide the PII necessary for the transaction and, if applicable, shipment of an ORCA Card. Please note, however, the following does not apply when you pay at an ORCA Retailer (See Section 10 below) or at a ticket vending machine. Any PII that you provide at a ticket vending machine to make payment with a credit or debit card is collected and processed under the ticket vending machine system, not the ORCA system.

6.2 When you pay by personal check, the following information is provided by you or may be collected from the face of a check: name; address; driver's license number; check amount; checking account number; and check routing number.

6.3 When you pay by credit or debit card for a single transaction, the following is provided by you or collected from the card: name; PIN number if debit card; billing address; and the credit or debit card number

and expiration date. An encrypted transmission of this information is sent to the credit card verifying and processing companies. The ORCA system only retains your name, billing address, expiration number, the last four digits of the credit card number and an authorization number generated for that transaction.

6.4 When you authorize recurring credit card transactions to "Autoload" ORCA Products on your ORCA Card, the following information is provided by you and stored in the ORCA system: name; billing address; credit card number and expiration date; and directions on when to charge your credit card. Your credit card information is stored in an encrypted database in the ORCA system. Each time a payment transaction is triggered, the necessary credit card information is sent via an encrypted transmission to the credit card's verifying and processing companies.

6.5 If you are purchasing an ORCA Card and request that it be shipped to you, your name, address and other shipping information will be collected and shared with the U.S. Postal Service.

6.6 If there is a problem processing an order, your PII may be used to contact you.

7.0 Information Related to the Use of ORCA Cards and Products

7.1 When an ORCA Card is presented to an ORCA reader device for fare payment or to check the card's status, the system collects the following information:

a. Date and time the card was presented.
b. Number from the reader device used.
c. I.D. of the Agency or Retail Revalue Site whose reader device was used.
d. Location of the reader device, if the device is at a fixed location (e.g. retailer; WSF gate, rail platform).
e. Vehicle and route numbers if the card is read by a device on an Agency vehicle.
f. Nature of the transaction (e.g. checking the status of ORCA Products on the card or payment of fare).
g. Amount/type of ORCA Product used.
h. Any transfer or incentives applied.

7.2 The ORCA Card itself contains a record of the last ten (10) uses of the card.

7.3 Information related to the ORCA Card's use is associated with the card's serial number. If you have provided PII linked to your card's serial number, the information about the use of the ORCA Card can be associated with your PII.

8.0 Information Residing on ORCA Cards

8.1 The card serial number and card verification number are printed on the ORCA Card.

8.2 The following information resides in an electronic form in an ORCA Card:

a. Information about the card properties (e.g. directory of entries and their sizes; expiration date; blocking status.
b. Type of card and:
    i. Passenger type expiration date (temporary RRFP)
    ii. Date of birth (if present)
    iii. Any eligibility for a personal care attendant, if RRFP Card
    iv. The I.D. number of the Business Account, if Business Account Card.
c. Zone fare preference pre-sets.
d. Autoload settings for automatic revalue of products.

e. Fare products loaded onto card including remaining E-purse and passes.
f. History of prior ten (10) trip transactions.
g. History of prior five (5) revalue transactions.

8.3 If present on the card, a passenger type expiration date and birth date are encrypted.

9.0 ORCA Websites and the Information Collected

9.1 The Agencies maintain two public websites for customer services related to the ORCA Program: www.orcacard.com and www.orcacard.biz.

9.2 Our servers automatically record and store information that a computer or browser sends whenever a person visits an ORCA Website, even if only to browse or download information. These server logs may include the following information:

a. Internet Protocol (IP) Address and domain name associated with your computer's connection to the Internet. The Internet Protocol Address is a numerical identifier assigned either to your Internet service provider or directly to your computer.
b. Type of browser, browser language and operating system used.
c. Date and time you visited an ORCA Website.
d. Website you visited prior to coming to an ORCA Website.
e. Pages viewed by users, the amount of time users spent on a certain page, search terms and other non-personally identifying information that may be collected as an ORCA Website is navigated.
f. One or more cookies that may uniquely identify your browser.

We also may collect statistical information about your use of the ORCA Websites, such as "clickstream data" and "user hits" which are visits and sessions that may be logged to determine which pages are visited most frequently.

9.3 When you visit ORCA Websites, your computer will receive one or more "cookies." Cookies are small text files placed on a user's computer and accessed by the ORCA Websites to recognize repeat users, to facilitate the user's ongoing access to and use of the website, and to compile data to improve the site and related business purposes. Most browsers are set up to accept cookies, but you can reset your browser to refuse all cookies or to indicate when a cookie is being sent. However, some ORCA Website features and services may not function properly if your cookies are disabled.

9.4 Although it may identify a user's computer, automatically collected information is not considered PII because it does not personally identify individuals. Automatically collected information is typically consolidated on a daily basis and kept at an aggregate level by the Agencies' contractor(s) responsible for providing the ORCA Websites. Such information may be used by the Agencies and their service providers to help understand how people are using the ORCA Websites and improve the value of the websites and the ORCA Program. Automatically collected information may be used to detect or attempt to prevent unauthorized intrusions on the ORCA Websites.

9.5 Personally Identifying Information (PII) will be collected on an ORCA Website only if you seek certain services and only if you choose to provide such information via the website. The PII required for ORCA-related services are described in other sections of this Privacy Statement. Should you seek a service that requires PII but you do not wish to provide PII via an ORCA Website, you may choose to provide the required PII by visiting an Agency customer service office.

9.6 When you send an e-mail or letter with questions or comments to the ORCA Program or an Agency,

or if you provide your contact information when ordering ORCA Cards, ORCA Products or services, the Agencies may retain these communications, and use your e-mail address and other information included in your correspondence in order to process your communications, respond to you and improve our services.

9.7 The ORCA Websites may have links to other websites, such as the Agencies' individual websites. When you link to one of these external websites, you are no longer on an ORCA Website and this Privacy Statement no longer applies. Instead, you are subject to the privacy notice and other terms of that external website.

10.0 ORCA Program Information Available to ORCA Retailers

10.1 An ORCA Retailer is equipped with a device that can check the status of ORCA Products on a card or load ORCA Products or a new adult ORCA Card purchased at that site. To enable accurate transfer of ORCA revenues from the Retailer, a report of all such transactions, by card serial number, is produced by the ORCA Program and regularly provided by an Agency to the Retailer..

10.2 A Retailer is prohibited from using any information received from the ORCA Program for any purpose other than performing its functions under its agreement with the Agencies.

10.3 If you provide PII to a Retailer (e.g. your name and a check, debit card or credit card) in connection with your payment for an ORCA Card or ORCA Product, such PII is not collected by the ORCA Program and is not covered by this Privacy Statement. The Retailer, not the Agencies, is responsible for the collection, storage, transmittal, safekeeping and use of that information.

11.0 ORCA Program Information Available to Business Accounts

11.1 A Business Account owns the Business Cards that are distributed to its employees, students or other program participants. The Business Account has a record of the serial numbers of all cards it has purchased and distributed. The card serial numbers may be linked by the Business Account to names and other PII that it may have.

11.2 The ORCA Program does not collect PII associated with the serial numbers of Business Cards unless you choose to register your Business Card. For example, an Agency will typically only know that it issued ORCA Business Card numbers 100 through 200 to a specific employer. The employer will know that it assigned Card #101 to a specific employee. The employer does not typically share the employee's name with the Agencies but may provide it to the Agencies for administrative purposes such as resolving questions about a card or investigating unauthorized use of the card or other business purposes.

11.3 A Business Account may obtain transaction data for a specific card serial number.

12.0 Use and Sharing of Information

12.1 Except as otherwise restricted in law or in this Privacy Statement, the Agencies plan to use and share all information collected through or generated by the ORCA Program for the purposes of fare media sales, fare collection, support of Business Account transportation programs, monitoring the functionality and performance of the ORCA Program, soliciting and receiving feedback, developing the ORCA Program, making reports on ORCA Card use and other ORCA-related activities or products, and for any other ORCA Program or Agency purposes.

12.2 The Agencies will not sell PII to other entities for their marketing purposes. The Agencies will only share PII with:

a. Agency employees, officials and contractors on a "need to know" basis for purposes of fulfilling

their duties and responsibilities.

b. Other persons or entities if it is reasonably necessary to:
   i. Satisfy an applicable law or regulation.
   ii. Respond (voluntarily or involuntarily) to a subpoena, court order or other legal process and requests by a governmental agency; and to protect the Agencies from any kind of potential harm (as an Agency perceives that potential in its discretion).
   iii. Enforce Agency terms of use and other provisions applicable under the ORCA Program or an Agency transportation service, including investigation of potential violations thereof.
   iv. Detect, prevent, or otherwise address fraud, security or technical issues.
   v. Protect against harm to the rights, property or safety of the Agencies, the users of their services, or the public, as required or permitted by law.

12.3 Persons or entities that receive information from the Agencies may be able to combine such information with other information they independently possess. The Agencies are not responsible for combining or any later use that may be made of information provided to others in accordance with this Privacy Statement.

13.0 Retention of Information

13.1 Information collected through or generated by the ORCA Program may be retained in the ORCA central system and at individual Agencies, on both active databases and in archive systems, and in electronic as well as hard copy form.

13.2 The Agencies will store all information related to the ORCA Program for as long as they believe it useful or required by applicable law.

14.0 Public Records

14.1 The Washington Public Records Act (Chapter 42.56 RCW) ("Act") applies to all records related to the ORCA Program including but not limited to: any data and reports related to the issuance, loading and use of ORCA Cards and Business Cards; PII that you provide; and the e-mails, comments and other communications between you and any of the ORCA Agencies. Generally public records are available for inspection and copying by the public but the Act exempts some records from mandatory disclosure. For example, the Act contains the following exemptions from mandatory disclosure.

RCW 42.56.330(4) The personally identifying information of current or former participants or applicants in a paratransit or other transit service operated for the benefit of persons with disabilities or elderly persons;

RCW 42.56.330(5) The personally identifying information of persons who acquire and use transit passes or other fare payment media including, but not limited to, stored value smart cards and magnetic strip cards, except that an agency may disclose personally identifying information to a person, employer, educational institution, or other entity that is responsible, in whole or in part, for payment of the cost of acquiring or using a transit pass or other fare payment media, and for the purpose of preventing fraud. As used in this subsection, "personally identifying information" includes acquisition or use information pertaining to a specific, individual transit pass or fare payment media.

Information regarding the acquisition or use of transit passes or fare payment media may be disclosed in

aggregate form if the data does not contain any personally identifying information.

Personally identifying information may be released to law enforcement agencies if the request is accompanied by a court order.

The Agencies reserve their discretion, if any, to release or withhold records in accordance with the Act.

14.2 The Agencies reserve the right to impose fees in accordance with the Act for responding to requests for inspection and copying of records.
14.3 In the event of a conflict between this Privacy Statement and the Public Records Act or other law governing the disclosure of records, the Public Records Act or other applicable law will control.

15.0 Information Security
15.1 The Agencies' security measures are intended to protect against unauthorized access to or unauthorized alteration, disclosure or destruction of information collected or generated under the ORCA Program. For example, steps have been taken to safeguard the integrity of their telecommunications and computing infrastructure, including but not limited to authentication, monitoring, auditing, and encryption. In addition, customer orders are processed through a secure server using advanced forms of encryption software. This means that all your PII entered online will be encrypted during transmission to maximize security protection. Because the ORCA Websites do not encrypt email, however, you should not send emails containing information that you consider sensitive.
15.2 Notwithstanding the above, this Section 15 and this Privacy Statement should not be construed in any way as providing business, legal or other advice, or warranting as fail-proof, the security of information provided by or submitted to the ORCA Websites or otherwise submitted to the ORCA Program or Agencies through customer participation in the ORCA Program. Due to the nature of Internet communications and evolving technologies, the Agencies cannot provide, and disclaim, assurance that the information you provide to them will remain free from loss, misuse, or alteration by third parties, who, despite the Agencies' efforts, may obtain unauthorized access.
15.3 If, despite the ORCA Program's information security measures, unencrypted "personal information" held by the Agencies was, or is reasonably believed to have been, acquired by an unauthorized person, the Agencies shall notify the subject of that personal information in accordance with RWC 42.56.590. For purposes of this Section, "personal information" has the same definition as it does in RCW 42.56.590(5) and (6).

16.0 Changes to or Deletion of Personal Identifying Information
16.1 The Agencies depend on the users of ORCA Cards and ORCA Products to update their own PII whenever necessary. You may use the ORCA Website or visit an ORCA customer service office to update your personal details and modify or terminate your ORCA Card registration or Autoload authorization.
16.2 You may request deletion of your name and other PII from the active ORCA database(s). Please understand, however, that it may be impossible to remove this information completely, due to system backups and records of deletions. In addition, if you request deletion of your PII, you will be unable to utilize associated features of the ORCA Website and possibly other services offered through our ORCA Programs, such as a registering an ORCA Card. The Agencies will fulfill a PII deletion request within a reasonable time.

17.0 NO WARRANTIES

THE AGENCIES HAVE ADOPTED PROCEDURES AND MEASURES THEY BELIEVE TO BE COMMERCIALLY REASONABLE TO PROTECT ANY INFORMATION COLLECTED FOR THE ORCA PROGRAM INCLUDING INFORMATION COLLECTED ON ORCA WEBSITES. HOWEVER, NO ONE IN THE AGENCIES GUARANTEES INFORMATION SECURITY OR WARRANTS THAT THE INFORMATION (INCLUDING BUT NOT LIMITED TO PII) COLLECTED IN CONNECTION WITH THE ORCA PROGRAM WILL REMAIN FREE FROM UNAUTHORIZED ACCESS OR DISCLOSURE, LOSS, MISUSE, ALTERATION OR THEFT AND THE AGENCIES EXPRESSLY DISCLAIM ANY SUCH OBLIGATION.

18.0 Governing Law and Venue

This Statement shall be construed in accordance with the laws of the State of Washington, without regard to any conflict of law provisions. Any dispute arising under this Statement shall be resolved exclusively by the state or federal courts sitting in King County, Washington that have jurisdiction over the matter.

19.0 Questions or Comments on this Privacy Statement

Please direct any questions or comments regarding this Privacy Statement to the ORCA Regional Program Administrator as follows:

E-mail: contactus@orcacard.com
Phone: 888-988-6722 / TTY Relay: 711 during regular business hours
Mail: ORCA Regional Program Administrator
401 S Jackson
Seattle, WA 98104

When we receive formal written questions or complaints at this address, it is our policy to contact the complainant regarding his or her concerns.

20.0 Changes to this Privacy Statement

20.1 This Privacy Statement may change over time. We expect most changes will be minor. Significant changes will be posted in the "News" footer located at the bottom of the ORCA Website pages. The date of the most recent revision of this Statement will be identified at the top of the page and prior versions will be kept in an archive for your review upon your request.

20.2 We will post changes to this Statement at least ten (10) days before they take effect. Any information we collect under the current Privacy Statement will remain subject to the terms of this Statement. After any changes take effect, all new information we collect, if any, will be subject to the new Statement.

Alternate formats are available upon request.

888-988-6722 (ORCA)
TTY Relay: 711
contactus@orcacard.com

ORCA Terms of Use

Last revised March 14, 2016

1.0 ORCA Program and Governing Terms and Conditions

1.1 Welcome to ORCA, which stands for One Regional Card for All. The ORCA Program allows you to participate in a regional fare payment system that enables you to use a single fare card when traveling on the public transportation services provided by the participating Agencies.

1.2 You may use cash to pay your fare and choose not to participate in the ORCA Program when you ride public transportation. If you choose to use the products and services provided by the Agencies under the ORCA Program (including but not limited to ORCA Cards, ORCA Products, ORCA Websites, and ORCA Customer Services), your use will be subject to and governed by these ORCA Program Terms of Use and the ORCA Program Privacy Statement (both are available at www.orcacard.com, www.orcacard.biz and at ORCA customer service offices) and such other terms and conditions, disclosures and consents that are contained in the ORCA Program Websites, forms, Business Account agreements and other written materials, all of which may be established, modified or withdrawn from time to time.

1.3 In addition to such ORCA Program-specific terms and conditions, your use of the ORCA Cards and ORCA Products is also subject to all applicable federal, state and local law, regulations, ordinances, codes and policies, including but not limited to each Agency's fares, tariffs, rates, prices, promotional programs, reduced fare programs, time and zone designations, routes, transfer policies, rules of conduct and other terms and conditions that apply to its public transportation services and which may be established, modified or withdrawn from time to time. Such other provisions applicable to public transportation service are available from the Agencies.

2.0 Definitions

As used in these Terms of Use, the following terms shall have the meanings indicated.

2.1 "Agency(ies)" means one or more of the following public transportation providers and the contractors and subcontractors which these Agencies, individually or collectively, have retained for purposes related to the ORCA Program.

a. Central Puget Sound Regional Transit Authority ("Sound Transit");
b. City of Everett ("Everett Transit");
c. King County ("King County Metro");
d. Kitsap County Public Transportation Benefit Area("Kitsap Transit");
e. Pierce County Public Transportation Benefit Area("Pierce Transit");
f. Snohomish County Public Transportation Benefit Area("Community Transit"); and
g. The State of Washington acting through the Washington State Department of Transportation, Washington State Ferries Division ("WSF")

For clarification, the term "Agency(ies)" does not include Business Accounts or Retailers.

2.2 "Associated Cardholder" means an entity or a person at least 18 years of age, other than the Primary Cardholder, who pays for the product or products on an ORCA Card.

2.3 "Autoload" means the Cardholder-authorized process for automatically loading ORCA Products on a registered ORCA Card and making a corresponding charge against the Cardholder's credit card to pay for the loaded Product.

2.4 "Business Account" means an entity other than an individual customer, including but not limited to an employer, educational institution or social service agency that purchases Business Cards and products for

distribution to its employees, students or other program participants according to the terms of an agreement with one of the Agencies.

2.5 "Business Card" means a type of ORCA Card issued to a Business Account for distribution by it to individuals who are eligible participants in the Business Account's transportation program.

2.6 "Card" means an ORCA Card.

2.7 "Cardholder" means a natural person to whom an individual ORCA Card has been issued by an Agency or to whom a Business Card has been distributed by a Business Account.

2.8 "Lead Agency" means one of the Agencies which, on behalf of itself and one or more of the other Agencies, signs an agreement with a Business Account for the sale of Business Cards and ORCA Products.

2.9 "Low Income" means a type of ORCA Card issued to an individual who is determined to be eligible in King or Kitsap counties for reduced fare based on income. A Low Income ORCA Card is not transferable.

2.10 "ORCA" means the trademarked acronym that stands for One Regional Card for All.

2.11 "ORCA Card" means the smart card that can be presented for payment of fare to ride train, bus and ferry services provided by, and in accordance with the terms established by, the Agencies. ORCA Card can mean cards issued to individuals and Business Cards, unless the context indicates it means one or the other.

2.12 "ORCA Customer Service(s)" means the facilities and services of one or more of the Agencies that exchange, with customers, information related to the ORCA Program and conduct sales of ORCA Cards and ORCA Products, including customer services counters, call centers, mail centers, Business Account support and ticket vending machines.

2.13 "ORCA Product(s)" or "Product(s)" means any transit fare payment option offered for sale within the ORCA Program, including, but not limited to, monthly or period passes and E-purse.

2.14 "ORCA Program" means the equipment, systems, facilities, ORCA Cards, ORCA Products, ORCA Websites, data, information, and any products and services related to the regional fare coordination and payment program implemented by the Agencies using smart cards as the common media for fare payment on their public transportation services.

2.15 "ORCA Websites" mean the following websites: Cardholder Website (www.orcacard.com) and Business Account Website (www.orcacard.biz).

2.16 "Personally Identifying Information" (PII)" means the following information when collected by the Agencies under the ORCA Program: a natural person's name; and, if combined with said name, such person's address, phone number, email address, date of birth, Regional Reduced Fare Permit-related information (as defined below) and photo, and check, debit card credit card information.

2.17 "Primary Cardholder" means the person who uses a Card for transportation services.

2.18 "Retailer" or "ORCA Retailer" means a retail business or other entity that, under an agreement with an Agency, is equipped with a device at which a customer may purchase ORCA Products for loading on an ORCA Card.

2.19 "Regional Reduced Fare Permit (RRFP)" means a type of ORCA Card issued to an individual who is determined to be eligible for reduced fare by one of the Agencies based on the individual's disability or age (age 65 and older). An RRFP ORCA Card is not transferable All RRFP ORCA Cards are registered Cards. A valid Medicare card is proof of eligibility for an RRFP.

2.20 "Youth Card" means a type of ORCA Card issued to an individual who is determined to be eligible for reduced fared by one of the Agencies based on the individual's age (6 to 18 years old). A Youth ORCA Card is not transferable.

3.0 Only Authorized ORCA Cards and ORCA Products Accepted

3.1 Only an Agency or a Business Account (e.g. your employer or another institution) or an authorized distributor may provide you with an authorized ORCA Card. You may not deface, alter, duplicate an ORCA Card or create a counterfeit ORCA Card. You may not load ORCA Products through an unauthorized means onto an ORCA Card or an unauthorized card. The Agencies do not intend to honor defaced, altered, duplicated or counterfeit cards or otherwise unauthorized cards or products.

3.2 The Agencies reserve the right to examine cards, confiscate any that are believed to be unauthorized or hold unauthorized products, and either deny transportation services to, or require payment in cash from, a person presenting unauthorized cards or products as payment for transportation service.

4.0 ORCA Products

4.1 The ORCA Products that may be loaded onto ORCA Cards represent prepaid fares on transportation services provided by ORCA Agencies. The three types of prepaid fares are:

a. Passes: the electronic equivalent of passes that are valid for use on the transportation service of one or more of the participating Agencies, depending on the type of pass.
b. E-purse: pre-paid value that may be used to pay a fare or a portion of a fare.
c. Multi-ride Ticket: Pre-paid rides that may be used to pay a fare on Washington State Ferries. A Multi-ride Ticket is route specific.

4.2 ORCA Cards are not, and do not represent, "accounts" or "deposits" and ORCA Products are not "money." They simply represent the transportation fare product for which you have already paid. You may not redeem ORCA Cards and ORCA Products for money or any product or service other than an applicable transportation service provided by an ORCA Agency. Sales of ORCA Products are final and nonrefundable, except for the limited refund of E-purse value available in accordance with Section 5.0.

4.3 Value added to an ORCA Card online, by mail, or by phone can take 24-48 hours to reach the ORCA card readers. After that time, you must tap at a reader to activate the value added. If you fail to tap the Card within 60 days, the E-purse value will become inactive and require the Cardholder to contact ORCA Customer Service to restore valid E-purse value (monthly pass value expires and will not be restored).

4.4 Payment shall be made to an Agency or to a Retailer for ORCA Products that are loaded onto an ORCA Card. The electronic record in the ORCA system shall be conclusive evidence of the ORCA Product value that was loaded on an ORCA Card and remains unused or unexpired.

4.5 Use of ORCA Products as a means of fare payment on a given trip will depend on the type of ORCA Product(s) loaded on the ORCA Card and on the policies and restrictions of the Agency providing that trip. For example:

a. Some products (passes are the most common) are specified to be usable at only one of the Agencies.
b. A pass product valued at less than the required fare plus E-purse value may be used in combination to cover the full amount of a single fare, if loaded on a single ORCA Card, except on Washington State Ferries.
c. A single ORCA Card can be used to pay for two or more people traveling together, except on Community Transit's *Swift* service. On Sound Transit, use of a single ORCA Card to pay for multiple riders is only accepted at a ticket vending machine, where the Cardholder may use E-purse value to purchase train tickets for companion(s).

4.6 If an ORCA Product or combination of Products is not usable or is not sufficient to cover the applicable fare, the Cardholder is required to make full fare payment by a means other than an ORCA Card.

4.7 The Agencies reserve the right to change fares at any time. To the extent value remaining on an ORCA Card is not sufficient, the Cardholder is required to make full fare payment by a means other than an ORCA Card.

4.8 The Agencies reserve the right to withdraw from the ORCA Program at any time and not accept ORCA Product(s) as fare payment. In that event, the Cardholder is required to make full fare payment by a means other than an ORCA Card.

4.9 The Agencies reserve the right to establish the terms for the use of the ORCA Card on their transit systems. Some Agency services allow or require a person to pay the fare prior to boarding a vehicle or entering a fare paid area and then requires the customer to present proof of payment while on board. (Examples of such service include Sound Transit's Link light rail and Sounder trains, Community Transit's *Swift* service King County Metro's RapidRide service, and Seattle Streetcar.) To show proof of fare payment on such services, the ORCA Cardholder is required to "tap" the ORCA Card at a yellow card reader before boarding or before entering a designated fare-paid area. (Tapping again within 5 minutes of your original card tap, at any reader on the platform or in the same

station area, will reverse the transaction.) Failure to tap before boarding or entering a fare paid area as required by these systems will subject the Cardholder to a fine. The Cardholder must tap the ORCA Card after getting off a Link or Sounder train, which ensures appropriate fare is validated. The failure to tap after getting off these trains will result in the Cardholder being charged the highest fare regardless of distance travelled.

5.0 E-purse

5.1 You may purchase E-purse value in full dollar increments with a minimum of $5 per load transaction. The maximum amount of E-purse value that may be held on an ORCA Card at any time is $300. When you add value to your ORCA Card online or by phone it can take 24-48 hours for the value to be available to be loaded onto your Card. You must tap the Card at an ORCA card reader within 60 days to activate the pass or E-purse value. After 60 days, if the Card has not been tapped, the E-purse value will become inactive and require the Cardholder to contact ORCA Customer Service to restore the valid E-purse value.

5.2 E-purse value on an ORCA Card is deducted to cover the full fare of a trip less: any applicable transfer value valid within two hours of the last use of the Card (except no transfer value is recognized on Washington State Ferries service); or reduced fares (e.g. youth fares; low income, the Regional Reduced Fare Permit). The amount of E-purse value remaining on your ORCA Card after a transaction will be displayed on the card reader. If the Card fails to accurately display the remaining value, promptly report problems to ORCA Customer Service. If you have an ORCA Business Card provided by your employer or other entity, report problems to the person or entity that gave you the Card.

5.3 If a ride costs more than the E-purse value remaining on an ORCA Card, the Cardholder must add sufficient cash to pay the full fare, unless an Autoload has been established as provided in Section 10.0.

5.4 A Cardholder with a registered, individual ORCA Card (i.e. not a Business Card) who opts to withdraw from the ORCA Program and surrenders said registered individual ORCA Card to an Agency may obtain a refund of the E-purse value that remains unused on the ORCA Card, less the applicable administrative fee (as specified in Section 15.0) for each E-purse refund processed. Upon surrender of the registered individual ORCA Card, it will be blocked and a refund, less the administrative fee, will be mailed to the Cardholder. If a transit voucher was used to purchase E-purse value, a refund of that value may be considered taxable income. The ORCA Agencies do not take responsibility for determining whether the refund is taxable. The Cardholder is responsible for reporting taxable income and obtaining tax advice.

5.5 A Business Account that surrenders a Business Card to its Lead Agency may obtain a refund of the E-purse value that remains unused on the Business Card, less the applicable administrative fee (as specified in Section 15.0) for each E-purse refund processed. Upon surrender of the ORCA Business Card, it will be blocked and a refund, less the administrative fee, will be mailed to the Business Account. The Agencies cannot distinguish between E-purse value purchased by the Business Account and E-purse value that may have been purchased by the individual Cardholder that used the Business Card. The Lead Agency will provide a refund of remaining E-purse value only to the Business Account that owns and surrenders the Card. The refund policy of the Business Account will govern whether the Business Account, in turn, forwards any of the refund to an individual Cardholder that claims to have personally loaded E-purse value onto the Business Card.

5.6 The ORCA Program complies with applicable Washington State Law for escheatment of unused E-purse value.

6.0 Card Registration

6.1 You may participate in the ORCA Program without providing any personal information. If you choose to register your ORCA Card or an ORCA Business Card provided to you by your employer or other entity, the card serial number will be linked to your Personally Identifying Information (see Privacy Statement for more details). If you choose to register your Card via the Cardholder Website, you will be required to set up an online ORCA account for which you also will be required to provide Personally Identifying Information.

6.2 In registering his/her Card and in creating an online "My ORCA login", the Cardholder agrees to: (a) ensure that all information provided is true, accurate, and complete; (b) promptly notify the Agencies in writing or via the ORCA Website of any changes to his/her name, address, and phone numbers; and (c) receive information about the ORCA Program via email and/or mailings from the Agencies.

6.3 A Cardholder with a registered Card may:

a. Access information about the Card's use and remaining value by calling ORCA Customer Service or via the Cardholder Website if he/she has an online "My ORCA login".
b. Report an ORCA Card lost, stolen or damaged and have the Card blocked and replaced in accordance with Section 8.0. Note: a damaged Card will display as lost/stolen in the Card's account history after it has been replaced.
c. Authorize the Autoload of new ORCA Products in accordance with Section 10.0.

7.0 Lost, Stolen or Damaged Cards

7.1 The Cardholder must take all reasonable care to prevent an ORCA Card from being defaced, altered, damaged, lost or stolen. The individual Cardholder or Business Account to whom a Card is issued bears the risk of loss if an ORCA Card is lost, stolen or damaged. A lost, stolen or damaged ORCA Card may remain valid and any ORCA Products loaded on such a Card may continue to be used for transportation services until the Product's value has been used or expires; provided, however, certain types of Cards may be blocked from continued use and replaced as provided in Section 8.0.

8.0 Blocking and Replacing Certain Cards

8.1 A registered ORCA Card or a Business Card that is reported as lost, stolen or damaged may be blocked and replaced as set forth herein. Unregistered Cards that are not associated with a business account cannot be replaced.

8.2 To block a lost, stolen or damaged registered ORCA Card and obtain a replacement, the individual to whom the Card was issued or the Associated Cardholder must report the missing or damaged Card. See Section 8.7 for lost, stolen or damaged Business Cards.

a. Submit the report for an Adult, Youth or Low Income ORCA Card online at www.orcacard.com, by calling ORCA Customer Service at 888-988-6722 / TTY Relay: 711; in person at an ORCA customer service office, or by mail with an ORCA Card Order form.
b. A Youth Card issued prior to June 6, 2012 may be replaced online however, if the website restricts a particular Youth Card from being replaced online, the Cardholder or Associated Cardholder will be directed to replace the Card in person or by mail. Requests submitted by mail require proof of age.
c. A Regional Reduced Fare Permit ORCA Card cannot be replaced online.
d. To obtain a replacement senior RRFP ORCA Card, the Cardholder or Associated Cardholder can go in person to any ORCA customer service office or contact the local transit agency for assistance. You may be required to provide identification.
e. A disabled RRFP ORCA Card can only be replaced in person at an ORCA customer service office.

8.3 A Card block will be initiated within 48 hours after the report of a missing or damaged Card. Reports may be submitted in person at an ORCA customer services office or by phone and processed during Agency business hours. Outside of regular business hours a registered Card can be reported lost, stolen or damaged online provided the Card is registered and the Cardholder or Associated Cardholder has a "My ORCA login". The risk of continued use of the E-purse and other ORCA Products by an unauthorized person remains with the Cardholder until the Card is blocked. Requests to block are final and may not be withdrawn.

8.4 A person who reports in person at an ORCA customer service office that a registered individual Card is missing or damaged may immediately obtain a replacement ORCA Card by paying the applicable administrative fee. Such replacement Card will be loaded with the unexpired pass product, if any, that had been on the lost, stolen or damaged Card at the time of the report. An E-purse on a blocked Card will be available on the next tap of the replacement Card, approximately ten (10) calendar days after the replacement Card is issued. The E-purse amount

that remains on the lost, stolen or damaged Card forty-eight (48) hours after the block is initiated in the ORCA system will be restored to the replacement Card via a remote revalue function. The Agencies are not responsible for any use of the E-purse product prior to the Card block taking effect.

8.5 A person who reports via the Cardholder Website or by phone that a registered individual ORCA Card is missing or damaged will be mailed a replacement ORCA Card in approximately seven (7) business days following report of the missing or damaged Card and payment of applicable administrative fee. The replacement Card will be loaded with the unexpired pass product, if any, that had been on the lost, stolen or damaged Card at the time of the report. An E-purse or multi-ride product from the blocked Card will be available on the next tap, approximately ten (10) calendar days after the Card was reported missing or damaged. The E-purse amount or unused rides from a valid multi-ride product that remained on the lost, stolen or damaged Card forty-eight (48) hours after the block was initiated in the ORCA system will be restored to the replacement Card via a remote revalue function. The Agencies are not responsible for any use of the E-purse or multi-ride product prior to the Card block taking effect.

8.6 To block a lost, stolen or damaged Business Card and obtain a replacement, the individual to whom the Card was distributed must report the missing or damaged Business Card to the Business Account that provided the card. The Business Account then must report it to the ORCA system via the Business Account Website or by calling the Lead Agency. A Business Card block will take effect when the report of a missing or damaged Card is processed in the ORCA system. For fastest processing, it is recommended that the report be submitted via the Card block function in the Business Account Website. Reports submitted by email, phone, or regular mail can only be received and processed during Agency business hours. The risk of continued use of the E-purse and other ORCA Products by an unauthorized person remains with the Business Account until the block takes effect. Requests to block are final and may not be withdrawn.

8.7 The Business Account will provide the replacement Business Card to the individual Cardholder and pay the Lead Agency any applicable fee. The unexpired pass product, if any, that had been on the lost, stolen or damaged Card at the time of the report will be loaded when the replacement Card is tapped after approximately two (2) business days. An E-purse or unused rides of a multi-ride product on a blocked Business Card will be restored when the replacement Card is tapped after approximately ten (10) business days. The amount restored will be the E-purse value or unused multi-rides which remained on the lost, stolen or damaged Card at the time the block was processed. The Agencies are not responsible for any use of the E-purse or multi-ride product prior to the Card block taking effect.

9.0 Blocking and Replacing Defective Cards

9.1 If an ORCA Card malfunctions, it will be blocked when it is surrendered at an ORCA customer service office or received at the ORCA Regional Mail Center (201 S Jackson St, MS KSC-TR-0108, Seattle WA 98104-3856).

9.2 You may obtain a replacement for the defective Card at the time it is surrendered by paying the applicable administrative fee. Provided, however, the Card will be replaced without a fee if the Card: (a) was surrendered to an Agency within twelve (12) months after it was issued to an individual or Business Account; and (b) the malfunction, as determined by an Agency customer service representative, was caused by a defect in design, material or workmanship and was not caused by misuse, an intentional act, negligence or damage (reasonable wear and tear excepted).

9.3 If the defective Card is surrendered at an ORCA customer service office, the replacement Card will be loaded with the unexpired pass product, if any, that had been on the defective Card at the time the Card was surrendered and the Card block was initiated. An E-purse or unused rides of a multi-ride product from the blocked Card will be available on the next tap of the replacement Card, approximately ten (10) calendar days after the Card was reported missing or damaged. The E-purse amount or unused rides of a multi-ride product that remained on the defective Card forty-eight (48) hours after the block was initiated in the ORCA system will be restored to the replacement Card via a remote revalue function. The Agencies are not responsible for any use of the E-purse or multi-ride product prior to the Card block taking effect.

9.4 If the defective Card was surrendered to the ORCA Regional Mail Center, a replacement Card will be mailed to the Cardholder within seven (7) business days of receipt of the Card and any applicable fee paid by check or

money order. The replacement Card will be loaded with the unexpired pass product, if any, that had been on the defective Card at the time the Card was surrendered and the block was initiated. An E-purse or multi-ride product from a blocked Card will be available on the next tap of the replacement Card, approximately ten (10) calendar days after the replacement Card is issued. The E-purse amount or unused multi-ride product that remained on the defective Card forty-eight (48) hours after the block was initiated in the ORCA system will be restored to the replacement Card via a remote revalue function. The Agencies are not responsible for any use of the E-purse or multi-ride product prior to the Card block taking effect.

9.5 A defective Card cannot be replaced online.

10.0 Autoload Program

10.1 A registered Cardholder or Associated Cardholder may authorize automatic reloading of ORCA Products and automatic payment by recurring credit card transactions. Autoload may be authorized for ORCA passes or E-purse. A Cardholder or Associated Cardholder may also authorize Autoload for a combination of E-purse and a monthly pass. The list of passes that can be loaded via Autoload is posted on www.orcacard.com. Autoload cannot be authorized on a Card provided by a Business Account.

10.2 In authorizing an Autoload, the Cardholder or Associated Cardholder agrees to:

a. Ensure that all information provided to ORCA is true, accurate, and complete.
b. Authorize the ORCA Agencies and their respective service providers to verify the information contained in the Autoload authorization.
c. Promptly notify the ORCA Agencies of any changes to the Cardholder's or Associated Cardholder's name, address, phone number(s), credit card account information and the other information provided in setting up the Autoload authorization. Changes may be submitted online or by using the printable Autoload Authorization form. IMPORTANT CAUTION: If the specified credit card expires or is otherwise cancelled and the payment fails, the Autoload authorization will be cancelled automatically.
d. Provide a valid credit card account and authorize a recurring transaction against said credit card account for the purchase the ORCA Products at the prices in effect at the time of each transaction.

10.3 If the Autoload of a monthly pass product (other than the King County Metro Access pass) is authorized:

a. A new monthly pass will be loaded automatically onto the ORCA Card the first time the Card is used in the new month, and the specified credit card will be charged. IMPORTANT CAUTION: The monthly pass product will Autoload with a fare-paying tap at an ORCA card reader. The full price will be charged regardless of when in that month the ORCA Card is first used.
b. The amount charged to the specified credit card will be based on the price in effect at the time the Autoload occurs, until and unless the Autoload authorization is terminated as provided herein. The price of the monthly pass product is subject to change by the Agencies.

10.4 If the Autoload Authorization specifies a monthly regional pass product, the face value of a Cardholder's specified pass product may become inadequate over time as a result of fare increases or loss of eligibility under a reduced fare program, i.e. youth, Low Income or RRFP. The Cardholder or Associated Cardholder must cancel the Autoload authorization on the original product and set up a new Autoload if a regional pass product with a higher face value is needed.

10.5 If Autoload of the King County Metro Access pass is authorized:

a. The credit card payment request will be initiated automatically on the 23rd of each month, until action is taken to cancel the Autoload.
b. If the credit card charge is successful, an email notification will be sent to the email on record for the Primary or Associated Cardholder and the pass purchase will be documented in King County's Accessible Services division.
c. If the credit card payment is not successful, the pass will not be purchased and the Autoload will be cancelled.
d. The price of the King County Metro Access pass is subject to change. If Autoload is authorized, the price in effect at the time the Autoload occurs will be charged, until and unless the Autoload is cancelled.

e. If the Access pass is authorized for Autoload the ORCA Card does not need to be tapped to set up, update or cancel the Autoload or to load the monthly pass.

10.6 If Autoload of E-purse value is authorized:

a. The amount to be added must be specified in full dollar increments of at least $5 but not more than $300.

b. The specified amount will be loaded automatically to the ORCA Card and the specified credit card will be charged when the ORCA Card is tapped to pay a fare and the E-purse value is insufficient to pay the fare of the current trip. IMPORTANT CAUTION: An Autoload of an E-purse will not be performed more than once per day or more than five times in a single month.

10.7 An Autoload authorization shall remain in full force and effect until it is terminated by the Cardholder, Associated Cardholder or by the Agencies as follows:

a. The Cardholder or Associated Cardholder may terminate his/her Autoload authorization by notifying the Agencies via the Cardholder Website or by submitting a signed written termination notice to the ORCA Regional Mail Center (201 S Jackson St, MS KSC-TR-0108, Seattle WA 98104-3856.) The Autoload termination notice shall specify an effective date that is at least ten (10) business days after the date of submittal of the form.

b. If the specified credit card expires or is otherwise terminated or if a credit card transaction authorized hereunder is rejected, reversed or otherwise fails to cover the price of an Autoload ORCA Product, that product may be blocked to prevent its further use. Under any circumstance, the Customer is liable for payment of the Autoload value if the credit card transaction failed to cover the price.

10.8 If an Autoload is terminated due to failure of a credit card transaction to cover the price of an Autoload ORCA Product, the Cardholder or Associated Cardholder may submit a new Autoload authorization online or by printing and submitting the Autoload Authorization form.

10.9 An Autoload may be set up on a Youth ORCA Card only by the Associated Cardholder.

10.10 Autoload of day pass products is not available.

11.0 Business Accounts and Business Cards

11.1 An employer, school, social service organization or other entity may apply to enter into a Business Account agreement with a Lead Agency to purchase ORCA Cards and ORCA Products for distribution to its employees, students, clients or other participants in its transportation program.

11.2 Each order for Cards and/or products that a Business Account submits and any other use of ORCA Program will be subject to the agreement and the prices in effect at the time of the order or use. A Business Account is responsible for reviewing the prices and fare information available from the Lead Agency before submitting each order; and shall be deemed to have agreed to pay the amount(s) displayed in the website order process by the act of submitting an order.

11.3 Although a Business Account remains the owner of the Business Cards after distribution, the Cardholder has the following privileges in connection with the use of an ORCA Business Card.

a. The Cardholder may present an ORCA Business Card, loaded with a valid, applicable ORCA Product, to an ORCA fare transaction processor as proof of payment of all or a portion of a required fare on transportation service operated by one or more of the ORCA Agencies. (Provided, however, an ORCA Product that is not sufficient to fully pay a fare will not be accepted as partial payment by the Washington State Ferries.) In all cases, a Cardholder will be required to make other payment to the extent a fare is not covered by an ORCA Product.

b. The Cardholder may individually purchase ORCA Products and load them on the Business Card in addition to whatever ORCA Products have been loaded by the Business Account.

c. The Cardholder may register his/her name and other contact information with the ORCA System and link such personal information to the serial number of the Business Card provided to him/her. Such registration does not give the Cardholder any ownership rights in the Business Card but does give the Cardholder the right to access the ORCA Cardholder Website to view the Card's transaction history

and current stored value and to modify travel zone preferences.

d. The Cardholder may not set up an Autoload on a Card provided by a Business Account.

11.4 The Business Account is responsible for implementation and enforcement of Cardholder Rules of Use and shall require that the Cardholder, as a condition of receiving a Business Card, sign written Cardholder Rules of Use that include:

a. A prohibition on the sale or transfer of the Business Card.

b. Notice that the Cardholder is required to pay any difference between a required fare and the value of the fare product loaded onto the Business Card.

c. Notice that any ORCA Products purchased by the Cardholder with his/her own funds and loaded on the Business Card, including but not limited to the E-purse, will become the property of the Business Account and any subsequent refund to the Cardholder would be the responsibility of the Business Account in accordance with its refund policy. Individuals are encouraged to purchase an individual ORCA Card if they have concerns about refund policies.

d. Notice that the ORCA System will record data each time the Cardholder presents a Business Card to an ORCA device to prove fare payment, to load a product on it or to review the amount and type of product on it. Such data will include but not be limited to the date, time and bus route or other location related to the Card being presented. Such data is owned by the ORCA Agencies but accessible to the ORCA System contractor(s) that operate it, the Business Account, and the ORCA Agencies.

11.5 The Business Account Website is the primary means by which the Business Account shall purchase ORCA Business Cards and ORCA Products, manage its Business Cards and obtain information about the use of said Cards. The Business Account agrees that it will use the Business Account Website when it is available and that each access and use of said website shall be subject to the Terms of Use and Privacy Statement that are in effect and posted on the Business Account Website at the time of such access and use.

11.6 The Business Account understands and agrees that uninterrupted access to and use of the Business Account Website is not guaranteed and agrees that it will contact its representative at the Lead Agency by email or phone if the website not available.

11.7 The Business Account understands and agrees that it is responsible for complying with any security standards specified by the Lead Agency which include but are not limited to controls on issuing, managing and rescinding access rights and passwords to the secured website pages for the Business Account.

12.0 Retailers

12.1 The sale of an ORCA Product or a new Adult ORCA Card at a Retailer is final and no refunds will be made by the Retailer or by the Agencies.

12.2 The Retailer does not sell ORCA Cards that require proof of age or eligibility.

12.3 The Retailer, not the Agencies, is responsible for the collection, storage, transmittal, safekeeping and use of payments and information you may provide to the Retailer in order to add value to an ORCA Card or to buy a new Adult ORCA Card.

12.4 The Retailer is not able to block and replace lost, stolen, damaged or defective Cards.

13.0 ORCA Websites

13.1 ORCA Websites and any ORCA Customer Services that require PII are not intended for minors, and we will not accept or request information from individuals we know to be under 18.

13.2 The ORCA Websites may provide links to various other websites, including each individual Agency's website. The Agencies are not responsible for each other's websites or for other "non-ORCA" websites. Any terms or privacy policies that appear on an Agency's website pertain to information collected by that Agency other than in connection with the ORCA Program. Your use of other websites will be subject to their respective terms and conditions.

13.3 Information on the ORCA Websites may change without notice.

13.4 If you create, or are issued, a password in connection with the ORCA Websites, actions or communications utilizing it will be attributed to you, even if someone else is using it. You need to keep your password confidential and not share it with anyone you have not authorized to use it on your behalf.

13.5 The viewing, printing or downloading of any content from an ORCA Website grants you only a limited, nonexclusive, revocable license for use solely by you for your own personal use and not for republication, distribution, assignment, sublicense, transfer, sale, preparation of derivative works or other non-personal use. No part of any content, graphic or document may be reproduced in any form or incorporated into any information retrieval system, electronic or mechanical, other than for your personal use. Except for the limited rights expressly granted herein, all right, title and interest in and to the Websites and all materials contained therein are retained by the Agencies. Your right to access ORCA Websites may be terminated at any time by the Agencies without notice.

14.0 Prohibited Acts

14.1 Use of any element of the ORCA Program is conditioned upon the user complying with all local, state and federal laws and regulations. Users shall not use the ORCA Program, including but not limited to the ORCA Websites, ORCA Cards and ORCA Products, in an unlawful manner or for an unlawful purpose. Without limiting the foregoing, users shall not do, or attempt to do, any of the following without the Agencies' express written permission in a non-electronic record: (a) attempt to access any area of an ORCA Website or ORCA equipment that the user is not authorized to access; (b) tamper with an ORCA Website or an ORCA Card or use any hardware or software intended to damage or interfere with the proper and timely functioning of an ORCA Website or ORCA Card; (c) intercept or collect any ORCA data or personal information from an ORCA Website, ORCA Card or ORCA equipment; (d) create a web page or site or computer application of any kind that deep links to or frames ORCA Websites, any page of said Websites, or any graphics, trademark or other proprietary information of any kind located on said Websites without the Agencies' express written permission; (e) use meta tags or any other type of hidden text utilizing ORCA Program or Agency names, trademarks or intellectual property rights on a website without the Agencies' express written permission; (f) alter, interfere with or deface information, graphics, trademarks or anything else on or obtained from an ORCA Website or ORCA Card; (g) use any robot, spider, scraper or other automated means or interface not provided by ORCA to access an ORCA Card, the ORCA Website or to extract data; (h) reverse engineer any aspect of the ORCA Websites or ORCA Cards, or do anything that might discover source code, or bypass or circumvent measures employed to prevent or limit access to, or change of, any area, content, value or code; (i) send or otherwise affect an ORCA Website, ORCA Card or any other service with software such as a virus, spyware or other code that could be illegal, harmful, deceptive or disruptive to the site, ORCA Cards, Cardholders, employers or others to whom ORCA Business Cards are issued, or to any Agency; or take any other action which might impose a significant burden (as determined by ORCA) on an ORCA Website or Card; (j) "frame" the ORCA Websites or otherwise make it look like ORCA or an ORCA Agency has a relationship to a person or entity that it does not actually have, or has endorsed someone or something for any purpose; or (k) take any action which imposes an unreasonable or disproportionately large load on an ORCA Website or ORCA Program network or other infrastructure.

14.2 Notwithstanding any provisions to the contrary, the cardholder may use an application to view his or her recent transaction history and card balance on his or her own ORCA Card. Neither ORCA nor its agencies make any warranty of any kind, expressed or implied, regarding applications that read and present data found on ORCA Cards or the accuracy of the information such applications may present.

14.3 Your messages and provision of information to the ORCA Websites or to one or more of the Agencies about the ORCA Program must be accurate, proper and related to the purposes of the ORCA Program. The following actions are prohibited: (a) making a misrepresentation such as misrepresenting one's identity, financial information, or eligibility for a program, benefit, fare or other service; and (b) posting or sending any defamatory, infringing, obscene, false, or unlawful material.

14.4 We hope you will provide free feedback to us to improve the ORCA Program. However, you are prohibited from providing feedback that infringes or violates the rights of others. By providing feedback, you grant a License to ORCA in your feedback and agree that no one has an obligation to pay for feedback or for the license to ORCA.

15.0 Administrative Fees

The following non-refundable fees will be charged:

15.1 Adult and Youth Card Issuance and Replacement - $5. Unless the Card is acquired during a promotional period or the Card is deemed by an Agency to be defective within 12 months of the date the Card was issued as provided in Section 9.0.

15.2 Low Income Card Issuance – no charge; Low Income Card Replacement - $5.

15.3 Regional Reduced Fare Permit (RRFP) Card Issuance and Replacement - $3. The fee will be waived for first-time conversion of an existing RRFP into an ORCA RRFP Card.

15.4 Refund Administrative Fee - $10.

15.5 Not Sufficient Funds (NSF) and other Fees. If a payment to the Agencies is not honored due to non-sufficient funds (NSF) or if for any reason a payment is negated or reversed, the Agencies may assess any late payment, NSF and collection fees to the maximum amount permitted by law.

16.0 Force Majeure

The Agencies and each of them shall have no liability for damages or any failure to perform due to circumstances or causes that are, directly or indirectly, beyond their control, including but not limited to: situations involving system failures or system malfunctions or unavailability; viruses or other harmful code; criminal acts; acts of nature; fire or water damage; acts of war, terrorism or the like; civil or public disturbances; acts of civil or military authorities; labor disputes and actions; accidents; and shutdowns for purpose of emergency repairs.

17.0 Reservation of Agency Rights

17.1 The Agencies and each of them reserve the right to suspend or deny an individual or Business Account from using any element of the ORCA Program, block an ORCA Card or ORCA Product, and recover all costs, expenses, losses, and damages incurred if: (a) the individual or Business Account fails to comply with these Terms of Use or any other applicable terms, policies, rules, laws and regulations; (b) a payment is not honored due to non-sufficient funds (NSF) or if for any reason a payment is negated or reversed; or (c) it is suspected that a Card has been altered, duplicated, counterfeited, stolen or used by an ineligible Cardholder.

17.2 When an ORCA Card is blocked in accordance with 17.1 above, the refund of any remaining value on the Card shall be at the absolute discretion of the Agencies, subject to such conditions as deemed fit including surrender of the Card and deduction of any amount due or payable by the Cardholder to the Agencies.

17.3 The authorized staff of an Agency shall have the right to inspect any Card and the Card data therein at any time.

18.0 NO WARRANTIES

18.1 THE AGENCIES AND EACH OF THEM MAKE NO REPRESENTATIONS, PROMISES, GUARANTEES, WARRANTIES OR ASSURANCES OF ANY KIND, EXPRESS, IMPLIED OR STATUTORY, REGARDING THE ORCA PROGRAM, INCLUDING BUT NOT LIMITED TO THE ORCA CARDS, THE ORCA PRODUCTS, THE ORCA WEBSITES, REPORTS AND OTHER INFORMATION OR OTHER THING OR SERVICE PROVIDED UNDER THE ORCA PROGRAM. ALL ORCA PROGRAM PRODUCTS AND SERVICES ARE PROVIDED ON AN "AS IS", "AS AVAILABLE" AND "WITH ALL FAULTS" BASIS. ANY USE OF ORCA PROGRAM PRODUCTS AND SERVICES, INCLUDING BUT NOT LIMITED TO ANY MATERIAL DOWNLOADED OR OTHERWISE OBTAINED THROUGH THE USE OF THE ORCA WEBSITES, IS DONE AT THE USER'S SOLE DISCRETION AND RISK.

18.2 TO THE EXTENT PERMITTED BY LAW, EACH AGENCY DISCLAIMS ALL WARRANTIES AND DUTIES OF EVERY KIND, EXPRESS, IMPLIED OR STATUTORY, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR CREATED BY TRADE USAGE, COURSE OF DEALING OR COURSE OF PERFORMANCE, ANY WARRANTIES OF QUIET ENJOYMENT OR NON-INFRINGEMENT AND ANY WARRANTIES OF WORKMANLIKE EFFORT OR LACK OF NEGLIGENCE. BY WAY OF EXAMPLE AND NOT LIMITATION, EACH AGENCY DISCLAIMS ANY WARRANTY

AND DOES NOT REPRESENT OR WARRANT THAT THE ELEMENTS OF THE ORCA PROGRAM (INCLUDING BUT NOT LIMITED TO THE ORCA WEBSITES, ORCA CARDS AND ORCA PRODCUTS) WILL BE UNINTERRUPTED, TIMELY, SECURE OR FREE FROM ERROR.

19.0 LIMITATIONS ON LIABILITY; EXCLUSIVE REMEDY

19.1 THE AGENCIES AND EACH OF THEM SHALL NOT BE LIABLE FOR ANY DAMAGES THAT ARE SPECIAL, CONSEQUENTIAL, GENERAL, INDIRECT, INCIDENTAL, OR PUNITIVE DAMAGES OR THAT ARE FOR LOSS OF USE, LOSS OF TIME, LOSS OF PROFITS, LOSS OF PRIVACY, LOSS OF DATA, LOSS OF GOODWILL, INCONVENIENCE, COMMERCIAL LOSS, LOSS OF ANTICIPATED SAVINGS, WASTED MANAGEMENT TIME OR LABOR, OR FAILURE TO MEET ANY DUTY (INCLUDING WITHOUT LIMITATION ANY DUTY OF LACK OF NEGLIGENCE OR WORKMANLIKE EFFORT), WHEN SUCH DAMAGES ARISE OUT OF OR ARE RELATED TO THE ORCA PROGRAM, EVEN IF ANYONE IN ANY OF THE AGENCIES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND EVEN IN THE EVENT OF A TORT (INCLUDING NEGLIGENCE, STRICT OR PRODUCT LIABILITY) OR VIOLATION OF CONTRACT OR POLICY.

19.2 IF THE AGENCIES OR ANY OF THEM BREACHES ANY DUTY OR AGREEMENT RELATING TO THE ORCA PROGRAM, THE EXCLUSIVE, AGGREGATE REMEDY WILL BE, AT THE OPTION OF THE ORCA AGENCY(IES): (A) CORRECTION, SUBSTITUTION OR REPLACEMENT OF ALL OR PART OF THE ORCA PROGRAM PRODUCTS OR SERVICES GIVING RISE TO THE BREACH, OR (B) A REFUND OF THE AMOUNT PAID FOR THE ORCA PRODUCT OR SERVICE CAUSING THE DAMAGE, WHICH AMOUNT WILL NOT EXCEED THE DAMAGES (OTHER THAN THOSE EXCLUDED ABOVE) ACTUALLY INCURRED.

19.3 THE LIMITATIONS ON LIABILITY AND REMEDIES IN THESE TERMS SHALL APPLY EVEN IF ANY REMEDY FAILS FOR ITS ESSENTIAL PURPOSE.

20.0 Applicable Law and Exclusive Jurisdiction

The laws of the State of Washington will govern all aspects of the ORCA Program, including but not limited to these Terms of Use, the Privacy Statement, and all performances and claims of every nature (including without limitation, contract, tort and strict liability) relating in any way to the ORCA Program, without giving effect to any principles of conflicts of laws. Any disputes regarding the foregoing shall be heard exclusively in the appropriate forum in Washington State. By using the ORCA Program, including but not limited to the ORCA Websites, ORCA Cards and ORCA Products, you consent to jurisdiction in a state or federal court sitting in Washington and waive any claim or defense that such forum is not convenient or proper, and consent to service of process by any means authorized by Washington State or federal law.

21.0 Copyright and Trademarks

21.1 All content on ORCA Websites and ORCA Cards and all data created under the ORCA Program, including but not limited to text, formatting, selection and arrangement of materials, the "look and feel" of the Websites, print or online images, graphics, video, logos, button icons, music, sounds, articles, copy, creative, trademarks and databases, is the property of the ORCA Agencies or their licensors, suppliers or service providers and is protected by copyright and trademark laws. No reproduction, modification, distribution, transmission, commercial use, reverse engineering, decompiling, disassembling, modification, re-posting to other websites, deep linking, republication, framing, display or use of any content on the ORCA Websites and ORCA Cards and all data created under the ORCA Program may be made without prior permission of the ORCA Agencies, except that you may print or make an electronic copy of the following: these Terms of Use and other disclosures or conditions on the site for your records and to the extent required by law, we hereby instruct you to do so. Additionally, you may print or download a copy of the printed public information such as fares, service locations and so on for your personal or employment purposes but not for other commercial purposes. It is our policy to terminate in appropriate circumstances user access for infringement.

21.2 The ORCA name, logo and slogans, as well as logos of the individual ORCA Agencies, are registered trademarks. Any copying or use not approved in writing in a non-electronic record by the Agencies is strictly

prohibited and all rights are reserved.

21.3 Nothing shall be construed as granting, by implication, estoppel or otherwise, any license or right to make commercial use of any ORCA trademark, intellectual property right or copyrighted material without the Agencies' prior written permission. Any unauthorized commercial use of these materials will violate the Agencies' intellectual property rights and will be subject to the Agencies' full legal rights and remedies.

22.0 Contact Information

Please direct any questions or comments regarding these Terms of Use to the ORCA Regional Program Administrator as follows:

ORCA Regional Program Administrator
E-mail: contactus@orcacard.com
Phone: 888-988-6722 / TTY Relay: 711 during regular business hours
Mail: ORCA Regional Program Administrator
401 S Jackson St
Seattle WA 98104

When we receive formal written questions or complaints at this address, it is our policy to contact the complainant regarding his or her concerns.

23.0 Changes to Terms of Use and ORCA Program

The ORCA Agencies retain the right to terminate or modify any of the Terms of Use and any other aspect of the ORCA Program at any time, at their own discretion and without notice to Cardholders, Business Accounts, or any other person or entity. Revised versions will be posted on the ORCA Website and will be available from any ORCA customer service office. Individuals and entities are encouraged to review from time to time these Terms of Use, the ORCA Websites and other Agency communications to be aware of any revisions. If the revisions are significant, a notice will be posted on the ORCA Cardholder Website homepage. The date of the most recent revision of these Terms of Use will be identified at the top of the page and we will keep prior versions in an archive for your review upon your request. Oral statements made by Agency employees or representatives will not constitute a change to these Terms of Use.

24.0 Notice to Users

Any Agency may provide notice to you, including (without limitation) legal notices, notices of amendments, and notice (as/if required) of breach of an information security system, by posting notice on www.orcacard.com, by emailing you, or by any other means that is lawful.

In order to allow us to obtain feedback, you also agree that the Agencies may contact you using any of the contact information you provide on your application to participate in the program, including by phone.

25.0 Notice to Copyright Agent

25.1 The ORCA Agencies respect the intellectual property rights of others and requests that users do the same. Anyone who believes that their work has been reproduced in an ORCA Website or a Card in a way constituting copyright infringement may provide a notice to the designated Copyright Agent for the site (specified below) containing the following:

a. An electronic or physical signature of a person authorized to act on behalf of the owner of the copyright interest.
b. Identification of the copyrighted work claimed to have been infringed.
c. Identification of the material that is claimed to be infringing and information reasonably sufficient to permit ORCA to locate the material.

d. The address, phone number, and, if available, an e-mail address at which the complaining party may be contacted.
e. A representation that the complaining party 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.
f. A representation that the information in the notice is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

25.2 Copyright infringement claims and notices should be sent to the attention of the ORCA Regional Program Administrator as follows:

ORCA Regional Program Administrator
E-mail: contactus@orcacard.com
Phone: 888-988-6722 / TTY Relay: 711 during regular business hours
Mail: ORCA Regional Program Administrator
401 S Jackson St
Seattle WA 98104

26.0 Notice of Availability of Filtering Software

The ORCA Agencies do not believe that the Site contains materials that would typically be the subject of filtering software. Nevertheless, you are hereby informed by the provider of this interactive computer service that parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist in limiting access to material that is harmful to minors. A report detailing some of those protections can be found at: http://www.ntia.doc.gov/ntiahome/ntiageneral/cipa2003/index.html (Children's Internet Protection Act: Report on the Effectiveness of Internet Protection Measures and Safety Policies).

27.0 NOTICE: NO HARVESTING OR DICTIONARY ATTACKS ALLOWED

THE ORCA AGENCIES WILL NOT GIVE, SELL, OR OTHERWISE TRANSFER ADDRESSES MAINTAINED BY THEM TO ANY OTHER PARTY FOR THE PURPOSES OF INITIATING, OR ENABLING OTHERS TO INITIATE, ELECTRONIC MAIL MESSAGES EXCEPT AS AUTHORIZED BY APPROPRIATE ORCA AGENCY PERSONNEL OR POLICIES. EXCEPT FOR PARTIES AUTHORIZED TO HAVE SUCH ADDRESSES, PERSONS MAY VIOLATE FEDERAL LAW IF THEY: (1) INITIATE THE TRANSMISSION TO ORCA (OR AN ORCA AGENCY'S) COMPUTERS OR DEVICES OF A COMMERCIAL ELECTRONIC MAIL MESSAGE (AS DEFINED IN THE U.S. "CAN-SPAM ACT OF 2003") THAT DOES NOT MEET THE MESSAGE TRANSMISSION REQUIREMENTS OF THAT ACT; OR (2) ASSIST IN THE ORIGINATION OF SUCH MESSAGES THROUGH THE PROVISION OR SELECTION OF ADDRESSES TO WHICH THE MESSAGES WILL BE TRANSMITTED.

Alternate formats of ORCA Terms of Use are available upon request.
888-988-6722
TTY Relay: 711
contactus@orcacard.com

Execution Version

FARE SYSTEM INTEROPERABILITY AGREEMENT

THIS FARE SYSTEM INTEROPERABILITY AGREEMENT (this "Agreement") is made as of this 15th day of October, 2014 (the "Effective Date"), by and among PORT AUTHORITY OF ALLEGHENY COUNTY, a body corporate and politic created under the provisions of the Second Class County Port Authority Act, as amended, having its principal office at 345 Sixth Avenue, Pittsburgh, Pennsylvania ("Authority"), WESTMORELAND COUNTY TRANSIT AUTHORITY, having its principal office at 41 Bell Way, Greensburg, Pennsylvania 15601 ("WCTA"), CITY OF WASHINGTON, a third class city, having its principal office at 55 West Maiden Street, Washington, Pennsylvania 15301 ("Washington"), BUTLER TRANSIT AUTHORITY, a municipal authority, having its principal office at 130 Hollywood Drive, Suite 101, Butler, Pennsylvania 16001 ("BTA"), MID MON VALLEY TRANSIT AUTHORITY, a municipal authority, having its principal office at 1300 McKean Avenue, Charleroi, Pennsylvania 15022 ("MMVTA") and FAYETTE AREA COORDINATED TRANSPORTATION, a local government agency, having its principal office at 825 Airport Road, Lemont Furnace, Pennsylvania 15456 ("FACT").

Recitals:

WHEREAS, Authority and Scheidt & Bachmann USA, Inc., a Delaware corporation having an address of 31 North Avenue, Burlington, Massachusetts 01803 ("S&B"), entered into a contract dated on or about March 13, 2009 (the "S&B Contract"), pursuant to which Authority purchased from S&B, and S&B agreed to provide to Authority, certain services and equipment for an automated fare collection system utilizing smart media cards known as ConnectCard or ConnecTix (each a "Smart Card" and together, "Smart Cards") on automated fare collection devices; and

WHEREAS, Authority and each of WCTA, Washington, BTA, MMVTA and FACT (each a "Regional Participant" and, collectively, the "Regional Participants") are parties to that certain Fare System Participation Agreement dated as of February 18, 2014 (the "Participation Agreement"), pursuant to which Authority and each of the Regional Participants agreed to set up and participate in the Authority Clearinghouse, as defined therein, to process transactions involving Authority's and each Regional Participant's customer's sales ("Smart Card Sales") and uses ("Smart Card Uses") of Smart Cards.

WHEREAS, Authority has implemented a central computer system (the "Authority CCS") which has the capability to manage data transfers and system interfaces with each Regional Participant's central computer systems (each a "Regional CCS" and, collectively, the "Regional CCSs"); and

WHEREAS, Authority and the Regional Participants desire to set forth the terms and conditions in this Agreement (i) to oversee and manage the flow of data, and provide certain interoperability, between the Authority CCS and each of the Regional CCSs; (ii) for Authority, through the Authority CCS, to deliver specific access to the Authority CCS, subject to certain requirements and limitations, to the Regional Participants; (iii) for restitution procedures to be used; and (iv) to document the respective roles, responsibilities and objectives of Authority and the Regional Participants with respect to the foregoing.

NOW, THEREFORE, in consideration of the premises and of the mutual benefits and covenants contained herein, the parties hereto, intending to be legally bound, agree as follows:

1. Recitals. The foregoing recitals are incorporated herein by reference and made a part of this Agreement.

2. Definitions. Except for terms specifically defined elsewhere in this Agreement, as used in this Agreement, the following terms shall have the meanings assigned to them below:

"Authority Customer" means an individual who has (i) purchased a Smart Card from Authority; (ii) used, or attempted to use, Stored Value on Authority's transit systems (regardless of whether such Stored Value was purchased from Authority or a Regional Participant); or (iii) used, or attempted to use, an Authority Transit Product on Authority's transit system (regardless of whether such Authority Transit Product was purchased from Authority or a Regional Participant).

"Authority Transit Product(s)" means any Transit Product which an individual has purchased for a fare or ride on Authority's transit systems and loaded on a Smart Card, including, without limitation, monthly passes, but excluding Stored Value and Smart Cards.

"Business Day" means any day other than a Saturday, a Sunday, legal holiday or other day on which Authority is authorized or required to be, or is, closed.

"CDRL" means that certain CDRL No. 23.8 dated as of February 13, 2012 for Back Office Services – Regional Interoperability Services Requirements attached hereto as Exhibit A.

"Customer" means either an Authority Customer or a Regional Customer, or both, as the context requires.

"Customer Support Services" means telephone, internet, electronic and other support services to resolve issues and problems for Authority Customers and Regional Customers, as applicable and as set forth in Section 4(a) of this Agreement.

"Interoperability Services" means (i) management and oversight by Authority of the Authority CCS to allow for the flow of certain information and transactional data between the Authority CCS and each of the Regional CCSs, provided, however, that Authority is not responsible for ensuring or managing the flow of such information and transactional data to the Regional CCSs; and (ii) delivery by Authority of specific access to the Authority CCS, subject to certain requirements and limitations, to the Regional Participants, each as further described in Section 3 of this Agreement.

"Modules" mean those software modules of, or used for, the Authority CCS that Authority, subject to certain requirements and limitations, will make available to each Regional Participant to use pursuant to, and subject to, this Agreement and which are set forth on Exhibit B hereto.

"Regional Customer" means an individual who has (i) purchased a Smart Card from a Regional Participant; (ii) used, or attempted to use, Stored Value on a Regional Participant's transit system (regardless of whether such Stored Value was purchased from Authority or a Regional Participant); or

(iii) used, or attempted to use, a Regional Transit Product on such Regional Participant's transit system (regardless of whether such Regional Transit Product was purchased from Authority or a Regional Participant).

"Regional Transit Product(s)" means any Transit Product which an individual has purchased for a fare or ride on a particular Regional Participant's transit system and loaded on a Smart Card, including, without limitation, monthly passes, but excluding Stored Value and Smart Cards.

"Reports" mean those computer-generated reports which Authority, subject to certain requirements and limitations, will make available for each Regional Participant to access or generate, which computer-generated reports are set forth on Exhibit C hereto.

"Stored Value" means cash amounts purchased and stored by Customers on their individual Smart Cards, which Stored Value can be used to purchase a fare or ride on Authority's or any of the Regional Participant's transit systems.

"Transit Products" means Smart Cards, Stored Value and other products which a Customer has purchased and received, or has purchased but has not yet received, for a fare or ride on Authority's or any of the Regional Participant's transit systems and store on their individual Smart Card, including, without limitation, monthly passes.

"Web Portal" means the web site operated by Authority through which an individual may purchase a Smart Card and/or other Transit Products for use on a Smart Card.

3. Interoperability Services; Access; Requirements.

(a) Modules and Reports. Subject to the various requirements and conditions in this Agreement, Authority will make available to each Regional Participant remote access to the Modules and Reports set forth in Exhibits B and C, respectively. For purposes of the foregoing, each Regional Participant will be able to: (i) modify, change or edit the data or information in the Modules and Reports where access is provided as set forth in Exhibits B and C; (ii) register Smart Cards for Regional Customers; and (iii) generate Reports.

(b) Information Download to Authority CCS. In order to ensure the efficient provision of the Interoperability Services, each Regional Participant shall automatically download all Smart Card Uses and Smart Card Sales to the Authority CCS on a daily basis. Each Regional Participant shall also provide, electronically, to Authority at the end of each business week any manual changes to Stored Value made by such Regional Participant in connection with one or more of its Regional Customers.

(c) Equipment. Each Regional Participant shall be solely responsible for purchasing, obtaining, maintaining, updating, upgrading, enhancing and utilizing all software, computer equipment, telecommunications equipment and telecommunications services necessary for such Regional Participant's CCS to continuously, securely and properly access the Authority CCS and the Modules and Reports on the Authority CCS. Authority shall have no obligation to purchase or provide any such equipment, software or services for any Regional Participant.

(d) Access Restrictions. Each Regional Participant shall, and hereby agrees to, (i) access only information on the Authority CCS for its own Regional Customers, and (ii) designate no more than two (2) individuals satisfactory to, and subject to the approval of, Authority to have access to the Authority CCS through such Regional Participant's CCS and shall notify Authority in writing of any changes to the person(s) having access to the Authority CCS, also subject to the satisfaction and approval of Authority. In no event shall more than two (2) persons from any Regional Participant have access to the Authority CCS through such Regional Participant's CCS at any time.

(e) Authority Policies. As a condition to accessing and using the Modules and Reports and/or the Authority CCS, each Regional Authority shall, and hereby agrees to, fully abide by the following Authority policies (the "Authority Policies") attached as appendices hereto, and any other requirements which Authority may subsequently issue for the use and access thereof:

- PAAC Corporate Information Security Policy (Appendix 1);
- PAAC Internet Acceptable Use Policy (Appendix 2);
- PAAC Firewall Policy (Appendix 3);
- PAAC Computer Security Policy (Appendix 4); and
- PAAC Third Party Service Provider Policy (Appendix 5).

Each Regional Participant hereby acknowledges and agrees that the Authority Policies and requirements are subject to change from time to time at the sole discretion of Authority.

(f) Additional Costs and Expenses. Any costs or expenses incurred in providing the Interoperability Services or access to the Authority CCS which relate to any specific Regional Participant(s), arise from a request of any specific Regional Participant(s) or arise from an action taken by, or omission of, a specific Regional Participant(s), and not Authority, shall be paid only by such Regional Participant(s).

(g) Additional Information and Modifications to a Regional Participant's Transit Products. Subject to Section 3(f) above, each Regional Participant shall provide Authority with at least sixty (60) days' written notice regarding any proposed changes to Transit Products, and/or tariffs, fares or prices of Transit Products, offered by such Regional Participant. Authority shall not be responsible or liable for any errors or omissions in connection with, or arising from, such changes to Transit Products, and/or tariffs, fares or prices of Transit Products, offered by such Regional Participant, but will endeavor to correct such errors or omissions as soon as is commercially and reasonably practicable.

4. Customer Services.

(a) Customer Support Services. Authority will provide Customer Support Services to Authority Customers. Each Regional Participant shall provide Customer Support Services to its Regional Customers. On a case by case basis and at the sole discretion of Authority, Authority may assist a Regional Participant in providing Customer Support Services to its Regional Customers.

(b) Restitution Procedures.

(i) Authority Restitution Procedure. Authority will, as appropriate, provide restitution services to Authority Customers in accordance with Exhibit D, Restitution Procedure.

(ii) Regional Participant Restitution Procedure. Within sixty (60) days of the Effective Date of this Agreement, each Regional Participant shall develop a restitution procedure for use with its Regional Customers that does not conflict in any manner with Authority's Restitution Procedure and submit the same to Authority and each other Regional Participant for approval prior to the implementation of said restitution procedure.

(c) Cooperation. In furtherance of providing support to Authority Customers and Regional Customers, Authority and each Regional Participant agree to cooperate and work together in good faith and when and as necessary to resolve Customer issues which may arise.

5. Confidentiality; Ownership and Use of Data.

(a) Confidentiality. Each Regional Participant hereby acknowledges and agrees that any individual or business information contained in the Authority CCS and any information about the Authority CCS, which is or may be accessible by a Regional Participant, is confidential information of Authority ("Authority Confidential Information"). Unless otherwise agreed to in writing by Authority, each Regional Participant agrees (i) except as required by law, to keep all Authority Confidential Information confidential and not to disclose or reveal any Authority Confidential Information to any person other than those employed by such Regional Participant, or on its behalf, who are actively and directly participating in the activities contemplated by this Agreement or who otherwise need to know the Authority Confidential Information for the purpose causing those persons to observe the terms of this Agreement, and (ii) not to use Authority Confidential Information for any purpose other than in connection with the purposes contemplated by this Agreement. Authority Confidential Information does not include, however, information which (A) is or becomes generally available to the public other than as a result of a disclosure by any Regional Participant or (B) became available to any Regional Participant on a nonconfidential basis from a person or entity, other than Authority, that is not bound by a confidentiality agreement with Authority and is not otherwise prohibited from transmitting the information to such Regional Participant. In the event that a Regional Participant is required by applicable law or regulation or by legal process to disclose any Authority Confidential Information, such Regional Participant agrees that it will provide Authority with prompt notice of such request(s) to enable Authority to seek an appropriate protective order or other appropriate remedy and/or, at Authority's sole discretion, waive compliance with the terms of this Agreement. In the event that such protective order or other remedy is not obtained, or that Authority waives compliance with the provisions hereof, such Regional Participant agrees to furnish only that portion of the Authority Confidential Information for which Authority has waived compliance or for which such Regional Participant is advised by written opinion of counsel is legally required to be provided and, upon Authority's request and at such Regional Participant's expense, to exercise best efforts to obtain assurance that the Authority Confidential Information will be accorded such confidential treatment.

(b) Ownership of Data/Information. As between Authority and the Regional Participants, individually and collectively, each Regional Participant hereby acknowledges and agrees that Authority

owns all right, title and interest in and to the information and/or data contained in or through the Authority CCS, regardless of the source of such information and/or data and that each Regional Participant shall only access and use such information and/or data for the purposes contemplated by this Agreement. In addition to the foregoing, Authority shall have the right to use and access all information, data and/or reports collected, prepared or generated by any Regional Participant in connection with this Agreement and stored in, or prepared from, the Authority CCS.

(c) Use of Data. Each Regional Participant hereby agrees (i) to use the information and data accessed from or through the Interoperability Services and/or the Authority CCS only for the purposes contemplated by this Agreement and for providing Customer Support Services to its Customers; (ii) not to delete any information or data in, or accessed from, the Authority CCS or to manipulate or use for any improper purpose any information or data in, or accessed from, the Authority CCS; and (iii) to notify Authority within twenty four (24) hours of such Regional Participant's becoming aware of the fraudulent or improper use of any such information or data, a Smart Card and/or a Transit Product.

6. Indemnification/Insurance. Each Regional Participant, on behalf of itself and its directors, officers, employees, agents and representatives, hereby agrees to and shall (i) defend, indemnify and hold Authority harmless for all claims, damages, costs (including, without limitation, reasonable attorneys' fees) and expenses arising from or as a result of the acts or omissions of such Regional Participant in using or accessing the Authority CCS and/or the management of access to and through such Regional Participant's Regional CCS, and (ii) if required by Authority at any time during the term of this Agreement, in Authority's sole discretion, provide a cyber-insurance policy and such other insurance policies, acceptable to Authority, and with Authority named as an additional insured and loss payee under such policy(ies), to cover potential claims, damages, costs (including, without limitation, reasonable attorneys' fees) and expenses arising from or as a result of the acts or omissions of such Regional Participant in using or accessing the Authority CCS and/or the management of access to and through such Regional Participant's Regional CCS.

7. Regional Participant Responsibilities. Each Regional Participant shall: (i) designate, maintain and service, and be responsible and liable for, each Regional Transit Product it issues or sells, and shall be responsible and liable for providing service to each of its Regional Customers, (ii) operate, maintain, enhance, upgrade and update its Regional CCS: (A) in accordance with the requirements of Sections 2 through 4 of the CDRL, and (B) to be fully compatible and current, at all times, with the Authority CCS, and (iii) implement policies, procedures and safeguards to ensure that only authorized personnel, in accordance with Section 3(d) of this Agreement, utilize and access the Authority CCS for legitimate transit purposes only and do not seek to access, utilize or manipulate the Authority CCS or any related hardware, software, equipment, information or data supporting same in any other manner, including, without limitation, any improper or unlawful manner, or for any other purpose not expressly set forth herein.

8. Term and Termination.

(a) Term. Except for any earlier termination in accordance with this Section 8, the term of this Agreement shall commence on the Effective Date and continue until the termination of the Participation Agreement, with respect to Authority and all Regional Participants, or shall terminate with respect to a Regional Participant in the event such Regional Participant's involvement in the Authority

Clearinghouse, as such term is defined in the Participation Agreement, terminates or is otherwise terminated pursuant to Section 8(b) of this Agreement (the "Term").

(b) Termination for Breach. This Agreement may be terminated with respect to any Regional Participant if such Regional Participant breaches its obligations under this Agreement, which breach(es) is not cured within thirty (30) days after receipt of written notice of the breach(es) from Authority. The Agreement shall continue for all remaining Regional Participants.

(c) Effect of Termination for a Regional Participant. Upon the termination of a Regional Participant, pursuant to either subsection 8(a) or 8(b) of this Agreement, Authority shall terminate such Regional Participant's access to the Authority CCS and the Modules and Reports, in addition to the other effects and procedures of termination set forth in the Participation Agreement.

(d) Termination by Authority. Notwithstanding anything else in this Agreement to the contrary, Authority may terminate this Agreement at any time upon one hundred eighty (180) days' written notice to all Regional Participants in the event Authority determines, in Authority's sole discretion, that this Agreement is, has become, or will become, unduly burdensome on Authority.

(e) Other Termination. This Agreement shall immediately terminate upon the agreement of Authority and all Regional Participants, set forth in writing and duly executed by Authority and all Regional Participants.

9. Representations and Warranties of Regional Participants. Each Regional Participant represents and warrants to Authority and each of the other Regional Participants as follows:

(a) This Agreement, when executed by such Regional Participant, shall be a legal, valid and binding obligation of such Regional Participant, enforceable against such Regional Participant in accordance with its terms.

(b) It has the power and lawful authority to enter into this Agreement and to perform the obligations hereunder.

(c) The execution and delivery of this Agreement by such Regional Participant does not violate, or constitute an event that with notice or lapse of time or both, would constitute a default under, any law, regulation, decree, order or agreement by which it is bound.

(d) All action necessary for the valid execution, delivery and performance by such Regional Participant of this Agreement has been duly and effectively taken, and evidence thereof, satisfactory to Authority, has been provided to Authority and all other Regional Participants.

(e) It shall comply with all Federal, state and local laws, regulations, policies, circulars and practices, as well as any changes thereto, which may be applicable to this Agreement, including, but not limited to, Pennsylvania's Right-to-Know Law.

(f) It shall not transmit or install, or allow the transmission or installation of, any malicious or disabling code that may damage, destroy or destructively alter the Authority CCS or any data

contained therein, including viruses, Trojan horses, worms, time bombs, backdoors, or mechanisms designed to permit it or any other person or entity to shut down or interfere with the operation of the Authority CCS.

10. Representations and Warranties of Authority. Authority represents and warrants to each Regional Participant as follows:

(a) This Agreement, when executed by Authority, shall be a legal, valid and binding obligation of Authority, enforceable against Authority in accordance with its terms.

(b) It has the power and lawful authority to enter into this Agreement and to perform its obligations hereunder.

(c) The execution and delivery of this Agreement by Authority does not violate, or constitute an event that with notice or lapse of time or both, would constitute a default under, any law, regulation, decree, order or agreement by which it is bound.

(d) All action necessary for the valid execution, delivery and performance by Authority of this Agreement has been duly and effectively taken, and evidence thereof, satisfactory to each Regional Participant, has been provided to each Regional Participant.

(e) Notwithstanding anything in this Agreement to the contrary, Authority is providing the Interoperability Services and access to the Authority CCS, the Modules and the Reports "AS IS" and makes no other warranties or representations of any kind or nature in connection therewith, either express or implied. EXCEPT AS EXPRESSLY SET FORTH HEREIN, AUTHORITY HEREBY DISCLAIMS ALL WARRANTIES, REPRESENTATIONS OR CONDITIONS OF ANY KIND EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTIES ARISING OUT OF THE COURSE OF DEALING OR USAGE OF TRADE. AUTHORITY ALSO MAKES NO WARRANTY OR REPRESENTATION THAT THE INTEROPERABILITY SERVICES OR THE AUTHORITY CCS, THE MODULES OR THE REPORTS WILL MEET ANY REGIONAL PARTICIPANT'S REQUIREMENTS OR WILL BE AVAILABLE ON AN UNINTERRUPTED OR ERROR FREE BASIS.

11. Resolution of Disputes. In the event of any dispute arising out of or relating to this Agreement, or its breach, promptly upon written notification by Authority or any Regional Participant to another Regional Participant or Authority, as applicable, as well as to Authority and all other Regional Participants, as applicable, regarding such dispute, the parties to such dispute, and Authority or any other Regional Participant that chooses to participate in the dispute resolution process at their own cost, shall use their best efforts to settle such dispute. To this effect, they shall consult and negotiate with each other, in good faith and understanding of their mutual interests, to reach an equitable solution satisfactory to both parties. If they do not reach such solution within a period of ninety (90) days after the issuance of such written notice, then the dispute shall be finally settled by either party commencing an action with the applicable court in Allegheny County, Pennsylvania, and Authority and all Regional Participants hereby consent to the jurisdiction of such courts.

12. Independent Contractor. Each Regional Participant acknowledges and agrees that the relationship which exists between it and Authority under this Agreement is that of independent contractor. No Regional Participant or Authority shall have any right, power or authority to enter into any agreement on behalf of, or incur any obligation or liability on behalf of, or to otherwise bind, Authority or any other Regional Participant, respectively. This Agreement shall not be interpreted or construed to create an employment relationship, an association, agency, joint venture or partnership between or among Authority and each Regional Participant or to impose any liability attributable to such a relationship upon Authority or any Regional Participant.

13. No Third Party Beneficiaries. No right, duty, obligation, nor any section, provision, condition or other term of this Agreement shall create or be construed to create or confer any express or implied third-party benefits or rights upon any person (including, but not limited to, Customers or other members of the general public) or entity (including, but not limited to, S&B) other than Authority and the Regional Participants as specifically set forth in this Agreement.

14. Survival. The terms of Sections 5, 6, 9, 10, 11 and 21 of this Agreement shall survive any termination of this Agreement.

15. Notices. All notices and communications concerning this Agreement shall be deemed given when made in writing and deposited in the United States Post Office addressed as follows:

(a) If to Authority:

Port Authority of Allegheny County
345 Sixth Avenue, Third Floor
Pittsburgh, PA 15222
Attention: Assistant General Manager
of Engineering and Technical Support

with a copy to:

Port Authority of Allegheny County
345 Sixth Avenue, Third Floor
Pittsburgh, PA 15222
Attention: Assistant General Manager of
Legal and Corporate Services/General Counsel

(b) If to WCTA:

Westmoreland County Transit Authority
41 Bell Way
Greensburg, PA 15601
Attention: General Manager/Executive Director

(c) If to Washington:

City of Washington
55 West Maiden Street
Washington, PA 15301
Attention: General Manager/Executive Director

(d) If to BTA:

Butler Transit Authority
130 Hollywood Drive, Suite 101
Butler, PA 16001
Attention: General Manager/Executive Director

(e) If to MMVTA:

Mid Mon Valley Transit Authority
1300 McKean Avenue
Charleroi, PA 15022
Attention: General Manager/Executive Director

(f) If to FACT:

Fayette Area Coordinated Transportation
825 Airport Road
Lemont Furnace, PA 15456
Attention: General Manager/Executive Director

16. Assignment. No Regional Participant shall assign this Agreement or any of its rights hereunder, without the prior written consent of Authority, which consent may be withheld for any reason whatsoever. Any assignment in contravention of this restriction shall be void and of no effect. Notwithstanding the foregoing, any merger, consolidation or similar combination of any two (2) or more of the Regional Participants is expressly permitted in connection with this Agreement; provided that the combined entity assumes, in writing, all of the obligations and liabilities of the consolidating or combining entities and Authority and the other Regional Participants are provided prior written notice and adequate assurance thereof.

17. Severability. Whenever possible, each provision shall be interpreted in such manner as to be effective and valid under applicable law, but in case any one or more of these provisions shall, for any reason, be held to be invalid, illegal or unenforceable in any respect, such invalidity or unenforceability shall not affect any other provision of this Agreement, and this Agreement shall be construed as if such invalid, illegal or unenforceable provisions had never been contained herein, unless the deletion of such provision or provisions would result in such a material change so as to cause the completion of these transactions to be unreasonable.

18. Amendment. This Agreement may not be amended, modified or extended, except by a written amendment duly executed by Authority and all Regional Participants. Authority and all Regional Participants hereby agree and acknowledge that amendments to this Agreement may be necessary, from

time to time, based upon actual operation of the Authority CCS and otherwise for the continued and efficient access to, and/or operation of, the Authority CCS. Authority and each of the Regional Participants agree to discuss and make any such necessary amendments in good faith.

19. Waiver. The failure of Authority or any Regional Participant at any time to enforce any of the provisions of this Agreement shall in no way constitute or be construed as a waiver of such provision or of any other provision hereof, nor in any way affect the validity of, or the rights thereafter to enforce, each and every provision of this Agreement. Any waiver of the breach of any of the terms and conditions of this Agreement by Authority or any Regional Participants shall be limited to the particular instance thereof and shall not be deemed to waive any other breach of such term or condition or of the other terms and conditions set forth herein.

20. Entire Agreement. This Agreement, together with each of the exhibits, other documents and agreements referenced herein, embodies the entire agreement and understanding among Authority and each of the Regional Participants and supersedes all prior agreements, discussions or negotiations among Authority and the Regional Participants relating to the subject matter hereof.

21. Governing Law; Jurisdiction and Venue. This Agreement shall be governed by the laws of the Commonwealth of Pennsylvania as they may from time to time be in effect, without giving effect to its conflicts or choice of laws provisions. Any suit or proceeding arising out of, or relating to, this Agreement shall be commenced only in a state or Federal court located in Allegheny County, Pennsylvania, and each party to this Agreement hereby consents to the jurisdiction of such court.

22. Counterparts. Authority and each of the Regional Participants may execute this Agreement in multiple counterparts, each of which constitutes an original, and all of which, collectively, constitute only one agreement. The signatures of Authority and all of the Regional Participants need not appear on the same counterpart. This Agreement is effective upon delivery of one fully executed Agreement or counterpart signed by Authority and each of the Regional Participants.

23. No Non-Drafting Party Interpretation. This Agreement shall be deemed to have been jointly developed and drafted by Authority and each of the Regional Participants. Authority and each Regional Participant has had the opportunity to consult with counsel regarding this Agreement and all have thoroughly read, understood and agreed to the terms and form of the same prior to the execution thereof. To the extent that any court of competent jurisdiction is called upon to interpret this Agreement, neither Authority, any individual Regional Participant nor group of Regional Participants shall be entitled to any benefit of interpretation as the "non-drafting" party or parties.

[Signatures appear on the next page.]

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the day and the year first set forth above.

ATTEST:

Diane M. Williamson
Signature

Assistant Secretary
Title
(Seal)

PORT AUTHORITY OF ALLEGHENY COUNTY

By: Ellen M. McLean
Signature

CEO
Title

Approved as to Form and Legality:

By: _____

Name Printed: Michael J. Ceth

Title: General Counsel

ATTEST:

_____
Signature

_____
Title
(Seal)

WESTMORELAND COUNTY TRANSIT AUTHORITY

By: _____
Signature

_____
Title

Approved as to Form and Legality:

By: _____

Name Printed: _____

Title: _____

IN WITNESS WHEREOF, the parties hereto have executed this Agreement as of the day and the year first set forth above.

ATTEST:

_____
Signature

_____
Title
(Seal)

PORT AUTHORITY OF ALLEGHENY COUNTY

By:_____
Signature

_____
Title

Approved as to Form and Legality:

By:_____

Name Printed: _____

Title: _____

ATTEST:

Signature

Dir. of Fixed-Rte. Serv.
Title
(Seal)

WESTMORELAND COUNTY TRANSIT AUTHORITY

By:_____
Signature

Executive Director
Title

Approved as to Form and Legality:

By:_____

Name Printed: John M. O'Connell

Title: Executive Director

ATTEST:

Christy S. Thomas

Signature

City Clerk

Title

(Seal)

CITY OF WASHINGTON

By: Brenda Davis

Signature

Mayor

Title

Approved as to Form and Legality:

By:_____

Name Printed: _____

Title: _____

ATTEST:

_____

Signature

_____

Title

(Seal)

BUTLER TRANSIT AUTHORITY

By:_____

Signature

_____

Title

Approved as to Form and Legality:

By:_____

Name Printed: _____

Title: _____

[Signatures continued on the next page.]

ATTEST:

_____
Signature

_____
Title
(Seal)

CITY OF WASHINGTON

By:_____
Signature

_____
Title

Approved as to Form and Legality:

By:_____

Name Printed: _____

Title: _____

ATTEST:

Kelly Stewart
Signature

PRIIT
Title
(Seal)

BUTLER TRANSIT AUTHORITY

By: [signature]
Signature

Executive Director
Title

Approved as to Form and Legality:

By: [signature]

Name Printed: Tiffany L. Burke

Title: Finance Manager

[Signatures continued on the next page.]

[Signatures continued from the previous page.]

ATTEST:

Signature

Finance Director

Title

(Seal)

MID MON VALLEY TRANSIT AUTHORITY

By: _____

Signature

Executive Director

Title

Approved as to Form and Legality:

By: _____

Name Printed: Diane A. Black

Title: Solicitor

ATTEST:

_____

Signature

_____

Title

(Seal)

FAYETTE AREA COORDINATED TRANSPORTATION

By: _____

Signature

_____

Title

Approved as to Form and Legality:

By: _____

Name Printed: _____

Title: _____

[Signatures continued from the previous page.]

ATTEST:

_____
Signature

_____
Title
(Seal)

MID MON VALLEY TRANSIT AUTHORITY

By:_____
Signature

_____
Title

Approved as to Form and Legality:

By:_____

Name Printed: _____

Title: _____

ATTEST:

_____
Signature
Chief Clerk
Title
(Seal)

FAYETTE AREA COORDINATED TRANSPORTATION

By:_____
Signature
Commissioners
Title

Approved as to Form and Legality:

By:_____

Name Printed: _____

Title: _____

EXHIBIT A
TO
FARE SYSTEM INTEROPERABILITY AGREEMENT

CDRL

See attached.

Submittal Coversheets

Port Authority

Project Name: Automated Fare Collection System — Agreement No: R08-01

Contractor/Vendor:	Scheidt & Bachmann USA, Inc.	**Date:**	2/13/2012
Address:	31 North Avenue Burlington, Massachusetts	**Submittal No.:**	
		QTY:	one original and one electronic copy
Telephone:	(781) 272-1664	**Re-submittal for:**	

CDRL NO:	0023.8	**CDRL Description:**	Back Office Services - Regional Interoperability Services Requirements

Supplier/Manufacturer/Sub Contractor:

☐ Initial Submittal ☒ Re-submittal ☐ Substitution Request

Note: Scheidt & Bachmann USA, Inc. hereby grants rights to use the information herein for evaluation by the Port Authority of Allegheny County (PAAC) employees ("Recipient"), and consultants deemed necessary for that purpose by Recipient, in conjunction with Agreement No. R08-01 between Scheidt & Bachmann USA, Inc. and the Recipient, dated March 13, 2009. Recipient shall not disclose or reproduce, either in electronic form or in hard copy form; the information contained herein without the prior written consent of Scheidt & Bachmann USA, Inc. to the extent that such non-disclosure does not conflict with or violate applicable Pennsylvania public records law(s) and/or applicable federal law(s).

Subject Identification; Plan and Specification References:

Agreement No. R08-01, Attachment A – Scope of Services

4.5.9 Regional Interoperability Services

The intent of this requirement is for potential interoperability between other regional agencies, assuming they use the same Smart Card and compatible AFCS system.

The Contractor shall provide central management and control systems necessary to perform the interoperability processes for a regional program. For purposes of this Agreement, "interoperability" is defined as the processing of all transactions to determine participants' end-of-day account position based on the transactions provided by participants by the end-of-day cut-off. The settlement process shall have the capability of occurring daily and is the reporting of end-of-day account positions. The Contractor shall document all clearing and related processes, and procedures for carrying them out.

The following is a summary list of the required clearinghouse capabilities:

- Provide transaction processing, and act as final transaction acquirer and processor of all system transaction activity
- Clear, reconcile and settle all transactions
- Manage data upload and download between the clearinghouse system and all Operators' computer systems
- Manage system interfaces
- Detect and manage fraudulent activity
- Provide the central database for system reporting, and provide standard and ad-hoc (user defined) reports to participants
- Maintain and operate all central clearinghouse system databases required for operations
- Provide and support system security and financial audit
- Provide access to all data and related databases.

Regional interoperability is based on a common stored value application and transfer business rules defined as follows:

- Each participating agency maintains their own tariff policies and products relative to their agency;
- All use of fare media between agencies will be addressed as transfer privileges.

Submittal Coversheets

Port Authority

Project Name: Automated Fare Collection System

Agreement No: R08-01

Deviations from Contract Documents:

N/A

Submittal Coversheets

Port Authority

Project Name: Automated Fare Collection System

Agreement No: R08-01

Notes or Comments :

N/A

Signed: _____ Date: 2/13/2012

By signing the submittal, the Contractor states that he/she has examined and checked the submittal for accuracy, completeness, quality and compliance with the requirements of the Contract before delivery to the PAAC.

Table of Contents

1 GENERAL 6

2 GENERAL INTEROPERABILITY CONCEPT 6

2.1 DEFINITION OF INTEROPERABILITY 7
2.2 INTEROPERABLE FARE MEDIA 7
2.3 INTEROPERABILITY OF STORED VALUE AND FARE PRODUCTS 9

3 IMPLEMENTATION OF INTEROPERABILITY 10

3.1 SYSTEM 10
3.2 FARE MEDIA AND RELATED SERVICES 11
3.3 FARE PRODUCTS AND POLICIES 11
3.4 SYSTEMS CONFIGURATION 12

4 OPERATIONS 14

4.1 GENERAL OPERATIONAL PROCEDURES AND POLICIES 14
4.2 PAAC'S RESPONSIBILITIES 14
4.3 RTA'S RESPONSIBILITIES 15

5 DATA PROCESSING, SETTLEMENT AND CLEARING 16

5.1.1 Settlement Process 16
5.1.2 Clearing 16
5.1.3 Financial Audit 17

6 OPTIONAL SOLUTIONS 22

7 ATTACHMENTS 23

8 REVISION HISTORY 23

1 General

This document identifies the requirements to perform the Regional Interoperability Services.

The document represents S&B's standard solution for a Smart Card System.

2 General Interoperability Concept

This document describes the design concept how to create and implement potential interoperability between PAAC and other regional agencies.

Under the interoperability the regional partners will establish business rules, commercial agreements and will operate the regional system.
S&B provides software solutions that enable the partners to implement the interoperable fare medium, perform settlement and exchange the necessary data per the requirements of **Agreement R08-01** between the Port Authority and S&B.

Under the interoperability the patrons will benefit from the use of the regional smart card (CONNECTCARD, CONNECTIX) at PAAC and all participating agencies:

- The CONNECTCARD holds a common Stored Value Purse and up to two fare products, e.g. passes or multi-trip tickets.
- The CONNECTIX holds a common Stored Value Purse. Alternatively, the CONNECTIX can be issued with one fare product that is only valid at the issuing agency. Agencies currently don't share fare products.

The patron will be able to load the Stored Value purse with money at field devices such as Sales Outlet Terminals, Ticket Vending Machines and Fareboxes and pay for fares at all participating agencies using Fareboxes and Validators. Passes and Multi-Trip tickets can be loaded onto the CONNECTCARD and used at the issuing agency. There are currently no shared fare products (passes, trip tickets, transfers) between agencies. The smart card is capable of storing transfers and electronically processing those using monies from the Stored Value Purse if there is an additional charge for the transfer.

Individual business rules and fare policies of each participating agency will be implemented in the agency-owned Central Computer and AFC systems. The operators will exchange transaction data required to determine their account positions and perform settlement of funds based on revenues collected and fares used with the interoperable fare media.

Further details regarding design and implementation of interoperability are described in the following sections below.

2.1 Definition of Interoperability

"Interoperability" is defined as the processing of all transactions to determine participants' end-of-day account position based on the transactions provided by participants by the end-of-day cut-off. (Agreement R08-01, Attachment A , section 4.5.9)

2.2 Interoperable Fare Media

The interoperable fare medium is the PAAC CONNECTCARD (MIFARE 1k Classic card) and the CONNECTIX (MIFARE Ultralight card). The following applies to the fare media:

a. The fare media used for the regional system will be the PAAC CONNECTCARD and the CONNECTIX.

b. Those media are encoded alike throughout the system. All partners will use the same smart card format and keys.

c. PAAC will act as the Card Issuer for all interoperable fare media in the regional system. All interoperable Smart Cards are procured through PAAC and issued from PAAC. PAAC and the RTAs will enter all necessary agreements and handling procedures to support Smart Card acquisition, distribution, operation and servicing. Card procurement by the RTAs is possible, but will require support by PAAC for release of card format and keys, and any procured cards need to be registered in the PAAC system.

d. PAAC as Card Issuer will service the cards. This includes smart card account management for registered users and any value /loss protections that may be offered under PAAC policies.

Refer to Figure 1 how the interoperable fare medium is shared between participating partners.

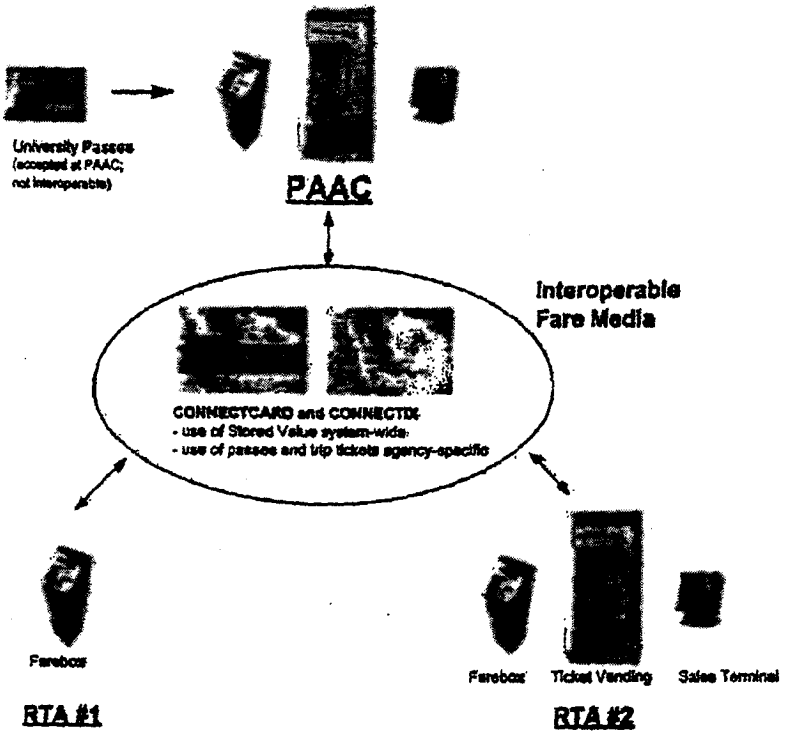


Figure 1 - Regional Fare Media

2.3 Interoperability of Stored Value and Fare Products

The requirements for Regional Interoperability define that it is based on a **common stored value application and transfer business rules** defined as follows:

- Sales, Re-load and Use of Stored Value at participating agencies. Stored Value can be reloaded system-wide at TVMs, Sales Terminals and fareboxes (if applicable) and be used at all participating agencies to pay fares and agency-transfers.
- Each participating agency maintains their own tariff policies and products relative to their agency. Sales of fare products (passes, trip tickets) will be performed at the individual agency where they apply and can be used; they are currently not shared between. For example, time-based passes will not be shared or result in any benefits for use at other agencies. Sharing of distribution and sales of such other fare products by multiple agencies or similar concepts currently do not exist and are not part of the interoperability requirements.
- Equipment design, functions and operations are currently not interoperable other than those required for the use of Stored Value. For example, shared operations such as credit card processing, fare media procurement and initialization are outside the interoperability concept required by the Agreement.
- Any future use of fare media between agencies will be addressed as transfer privileges. Currently, no such transfers between agencies exist. The capability to provide those transfers between agencies for future fare policies exists.
- The Smart Card user can add stored value and order automated stored value reloads through PAACs smart card account management system and web portals.

3 Implementation of Interoperability

The following items describe the basic concept of interoperability:

3.1 System

1. Each of the participating agencies operate their own individual and compatible AFCS system. Refer to Figure 2.
2. PAAC CCS (Central Computer System) system will be the CCS and interoperability office for all RTAs. All data required to operate Stored Value will be exchanged between PAAC and the participating agencies as follows (refer to Figure 3). The PAAC CCS will manage the data transfers and systems interfaces with the RTA CCS(s) by means of automated and scheduled FTP file downloads over a secure data line (e.g.bi-directional IP with data encryption at a min. 3DES 128 bit):
   a. Hotlist support files will be created at the PAAC CCS, duplicated into the RTA CCS's, downloaded from the RTA CCS into the RTA end devices, and processed by those end devices accordingly
   b. Actionlist support files for smart card actions to be performed (e.g. load value, block card etc.) will be created at the PAAC CCS, duplicated into the RTA CCS's, downloaded from the RTA CCS into the RTA end devices, and processed by those end devices accordingly.
      Action lists are updated to ensure that there is no duplication of loading the fare. Each action list item has a unique ID. The IDs of the most recently performed action list IDs is stored on the card. The end device will read the most recently performed IDs from the card first. If a pending entry was already executed, it will not be executed twice.
   c. The daily shift file upload will reconcile all executed action list entries and renew the action list for the devices.
   d. Transaction files (Device Shift Files) will be generated by the RTA field devices and uploaded to the RTA CCS. Shift files will be copied at the RTA CCS and copy duplicated onto the PAAC CCS, where they will be processed. All embedded device transaction data from RTA devices will be stored in PAAC CCS database to facilitate settlement and smart card customer support and account management.
   e. University Passes are interoperable with the Port Authority Fare Collection system under the PAAC University Pass program and will be used only on the PAAC system. Positive lists (lists with University Pass card #s) will be generated by the PAAC CCS and downloaded into PAAC devices only.
3. Revenues for Stored Value Sales are collected by each individual agency who operates and owns the particular devices where sales or reloads are being made.
4. Fraudulent Activity will be detected and managed as follows:
   a. Shift files with transactional data transmitted from devices to the CCSs are CRC protected and secured. If manipulated or corrupted the CRC will be invalid, those files will not be processed by the receiving device.
   b. Shift files with transactional data are sequentially numbered, this sequence number to be known by the CCS. Manipulated, duplicated or corrupted shift files will not be processed.
   c. Smart cards are secured with keys. Attempt to manipulate the data on the card will result in CRC error, those cards will no longer be accepted.
   d. Support Files (Hotlist, Actionlist) transmitted between the CCSs and devices are CRC protected and secured. If manipulated or corrupted the CRC will be invalid, those files will not be processed by the receiving device.
   e. Data between PAAC's CCS and RTA CCS's respectively devices are to be transmitted via secure and private networks. They must be secure against unauthorized access through the outside. Implementation of appropriate means available by the IT systems deployed (virus scanners, security policies, password protection, logging and audit trails) will prohibit unauthorized access to data. Governing policies for this data exchange are established by PAAC and the RTA's.

Data can be recovered from the devices at the RTAs if shift files are corrupted in the same way as PAAC would recover them:

1. In case of failure of the primary device memory a copy of the shift data is stored on a backup module. When the computer has to be replaced the old backup module will be re-used and the data transferred into the new primary memory.
2. If both primary and backup memory were to fail w/o the end device being able to upload the data to its CCS, the data is permanently lost. However, the use of redundant memory reduces the likelihood of data loss to a lowest possible minimum.

3.2 Fare Media and Related Services

1. All interoperable cards should be acquired by the Card Issuer (PAAC). The Card Issuer will issue those cards through their sales and distribution network provided under the Agreement, which includes Sales Outlet Terminals, TVMs and Web Portals. It is possible for RTAs to obtain cards from PAAC for issuing and distribution under agreement with PAAC, or to procure their own fare media with the following constraints:
    - Same card specifications, same encoding format.
    - Artwork may be individual
    - PAAC to share their SC keys with RTAs to allow procurement
    - Files with S/Ns for cards procured by RTAs must be imported into the PAAC CCS to allow Account Management and Registration with PAAC
    - Ensure control of MIFARE S/Ns to avoid duplicates – Currently, this can only be guaranteed when procuring from the same manufacturer.
2. The Card Issuer will subsequently service all smart card accounts and populate the card inventory database necessary to operate such smart card management. Refer to Figure 5.
3. Customer Service and card management for Interoperable Smart Cards is performed by PAAC or designated contractor(s) in accordance with existing PAAC business rules and currently established systems by PAAC. Such smart card account management functions including related generation of hotlists and action lists is performed at the PAAC CCS and connected workstation(s).
4. All cards in the system will have the same smart card keys. The PAAC smart card format provides a free memory area between field "pointer of last usage history" and "S&B security information" in logical sector 0 (phys sector 2/3, block 0), of which 8 bit can be used to encode an agency ID (value for PAAC = 0).
5. For all interoperable cards the PAAC RTAs can use Stored Value and product slots provided those are available and not already filled with active or pending products.
6. In the PAAC system all cards will be manufactured with PAAC keys and issued through PAAC.

3.3 Fare Products and Policies

1. Stored Value at Smart Cards can be re-loaded by the participating agencies.
2. Stored Value can be used to pay for the fare (single rides) throughout the area.
3. Stored Value is non-transferable, meaning it can only be used to pay for fares (single rides) and cannot be used as form of payment for fare or other products (passes, tickets).
4. The Stored Value purse on the existing PAAC Smart Card types and fare classes is the common fare element to implement interoperability. PAAC's currently existing business policies and rules for the use of this Stored Value purse apply for all RTAs.
5. PAACs Stored Value purse comes with two product types Full Fare and Half Fare per PAAC's fare policy and business rules. Other participating agencies need to implement fare policies for the acceptance of both Stored Value product types. Fares that are deducted from the Stored Value purse may be different at

each RTA, same applies for reduced fares at RTAs where they exist. A holder of a Reduced Fare card may be eligible to use this reduced fare card at all participating agencies with the understanding that PAAC has reduced fares in its fare policy but not all partners may offer reduced fare. In that case, the applicable (full) fare will be charged.

6. For example, there is no way to distinguish a Senior Citizen with a reduced fare card using his card at two partners that have different age limits for eligibility.
7. Certain privileges associated with the PAAC CONNECTCARD (e.g. Full Fare / Half Fare Stored Value) may or may not be transferred to the RTAs. The RTAs may, as defined in their own fare policies, accept or reject these product types.
8. PAAC and the RTAs currently allow no transfers between agencies. Future interagency transfers are time based. The system will allow transfers from one agency to another agency during a defined timeframe, called "Transfer Time". This "Transfer Time" is determined by the agency who issues this transfer. Within each agency the system will allow for a parameter "Transfer Time", which applies within each agency system-wide, but may vary between agencies. Transfer fares can be free or step-up fares based on route-route relations and fare class paid by cash for paper transfers or with Stored Value paid by the interoperable smart card.
9. Local transfers within one RTA can be stored and processed on the CONNECTCARD, or processed on paper-transfers. Interagency transfers apply for Stored Value use only.
10. PAAC's fare products can be added to the interoperable CONNECTCARD, RTA specific fare products can also be added to it.
11. Under this interoperability PAAC and the RTA's share no time based or ride based passes nor do the RTA's share these passes with each other.

3.4 Systems Configuration

The systems contain certain critical data indexes that have to be unique throughout the system. Those critical indexes are Short Device ID, Short Ticket Type ID, Short Route / Location ID, and they are unique indices and are to be the same in each of the CCSs of the participating partners. The data needs to be maintained at each of the CCSs by the operator(s) of the AFC systems, the system currently does not provide means to automated data exchange and transfer (copying of ID data).
For each Short ID, there is a Long ID and related subject information in a database record. The Long ID is unique for each agency, duplicates of the Long ID between the agencies can exist, but the Short ID is unique throughout the system because it is stored on the smart card that is shared and relevant for data processing, transfers and reporting. Duplicates of Short IDs will lead to errors in processing and settlement.

For example: Two agencies may have bus route #1. Consequently, the Long IDs in each of the CCSs would be "1", while only one agency could use the Short ID "1" and the other would have to have a different value. Short IDs are used for calculation of transfer based on relations between bus routes (last route – current route relation), therefore they cannot be overlapping. As part of the regional system design the Short ID ranges for each agency would be reserved.

Another example: Two agencies may have a device #1 in their fleet. Also here, the Long ID would be identical. For reporting purposes in the Settlement report and for customer service purposes the vehicle would have to be associated with an agency and therefore the Short Device ID would be unique throughout the system.

To implement interoperability the following minimum requirements apply:

1. Devices of the regional system must have their own unique Short Device ID. Upon delivery of the PAAC AFCS system S&B will provide a range of Short Device IDs that can be shared between and allocated to participating RTAs.

2. Ticket Types of the regional system must have their own unique Short Ticket Type ID. Upon delivery of the PAAC AFCS system S&B will provide a range of Short Ticket Type IDs that can be allocated to and shared between participating RTAs. Each RTA will own their own range of IDs.
3. Ticket Type IDs for interoperable fare products (Full Fare Stored Value, Half Fare Stored Value) must be maintained in the CCSs for all participating agencies.
4. Short Route/ Locations of the regional system must have their own unique Short Route/ Location ID. Upon delivery of the PAAC AFCS system S&B will provide a range of Short Route/ Location IDs that can be allocated to and shared between participating RTAs.
5. All devices must be maintained in the PAAC CCS, in addition to the CCS of the participating agency where they belong. This is necessary for customer service and transaction settlement.
6. If reports for transactions on RTA specific products other than interoperable fare products are required at the PAAC CCS, then those Ticket Types must be maintained at the PAAC CCS in order to populate the product names on the reports.
7. The Central computer for each agency maintains identifiers for device types, that are stored in Device Classes. For example, a standard farebox is a Device Class, or a TVM is another one. Those Device Classes are used in various reports for sales and usage statistics. To distinguish between the agencies in the Settlement Reports the Device Classes for device types of each participating RTA will get their own device class in order to allow for settlement of transactions and reporting. For example, fareboxes from PAAC may have assigned device class 501, fareboxes for RTA #1 may get 510, fareboxes for RTA #2 may get device class 511 etc..

4 Operations

4.1 General Operational Procedures and Policies

In addition to above, the following general requirements to operational procedures and policies apply:

1. PAAC and the RTAs are responsible for establishing all operational policies with PAAC, agreements and/ or Contracts necessary to operate the regional system and exchange data and information and allow for the use of the Smart Card as common fare media.
2. The RTAs and PAAC are responsible for installing and configuring the data communication infrastructure between the RTA system and PAAC CCS system and make it available to the Contractor prior to testing, integration and installation of RTA equipment.
3. The RTA's systems will connect to PAAC's system through a network. The network is provided by PAAC and the RTAs. S&B strongly recommends a secure line.
4. PAAC and the RTAs are responsible to establish appropriate means to secure data and access to their IT systems deployed against unauthorized use and access to data by using the tools and software provided by the Contractor(s) under the appropriate agreements.

4.2 PAAC's Responsibilities

1. Share the CONNECTCARD Smart card keys or provide access for injection of smart card readers to the participating agencies and their Contractors.
2. PAAC CCS system will be maintained and made available by PAAC if and as needed to the RTAs and S&B.
3. PAAC will be responsible to maintain any RTA data as required to implement interoperability.
4. Upgrades to support the additional capacity requirements on PAAC CCS system will be the responsibility of PAAC.
5. User IDs for probing cards will be maintained by whoever is creating or ordering those cards. If RTA probing cards are supplied by PAAC, then PAAC is responsible to maintain additional user ID's, access conditions etc. in the CCS after the initial configuration was performed by the Contractor.
6. PAAC is responsible to maintain additional device ID's of RTA devices in the CCS after the initial configuration was performed by the Contractor.
7. If required by operational policies PAAC will communicate with RTAs to update systems with windows updates and patches.

8. PAAC will notify S&B about such required upgrades to any and all software in advance as long as contractual obligations exist by S&B to the RTA's.

9. If required by operational policies all changes to Contractor-provided software must be notified to PAAC by the RTA before being implemented, together with an implementation plan. The purpose of this provision is to allow PAAC maintain compliance with their operational requirements.

4.3 RTA's Responsibilities

1. RTAs must provide PAAC with their fare structure and business rules and policies for customer service/support in a timely manner to support the project schedule.

2. The RTA will share the wireless encryption keys with PAAC.

3. PAAC may obtain from the RTAs copies of test reports as required to support the integration of RTA equipment into PAAC's system.

5 Data Processing, Settlement and Clearing

As stated above, all transactions generated by AFCS field devices will be uploaded and processed by the CCS of the particular agency. Copies of the shift files from RTAs will be sent to the PAAC CCS.
The PAAC CCS will act as final transaction acquirer and processor of all transactions throughout the system. In particular, all transactions related to the interoperable fare products Stored Value will be processed and stored in the PAAC database, which becomes the central database for all transactions within the region for the participating agencies.

5.1.1 Settlement Process

1. The settlement process will be based on settlement reports from the PAAC CCS. The RTAs will have access to the data generated by their own systems by the same reports so that they can verify the final settlement statements.
2. Settlement reports will be generated by PAAC to produce summaries of Stored Value Sales and Usages. Those reports shall be archived for the reporting period, which is to be defined and agreed on by PAAC and the participating agencies.
3. The sum of totals over the total of all cards and all fare classes for card sales and usages for Stored Value of a participating agency identifies the settlement balance for each agency. A positive balance identifies excess revenue over fares used. A negative balance shows an excess of fares used over revenues collected.
4. The PAAC CCS will provide settlement reports to settle transactions. The following pre-programmed reports provided under the Agreement will be used for settlement:
   a. Transaction Detail Report (#1003) – used to verify individual transactions
   b. Detail Sales Summary – used to summarize Stored Value Sales of a particular agency (Use of the filter <Device Class> will select the selling devices from a particular agency, and the filter <Ticket and Pass Type> will allow to select only the interoperable Stored Value product types.
   c. Settlement Report - used to summarize Stored Value usage of a particular agency and specifically developed for settlement for this purpose.
5. Settlement ends in a consolidated statement that defines whether the RTA owes revenue to PAAC or PAAC owes revenues to the RTA. PAAC will generate this statement based on the AFC reports within their own business system outside the AFC system.

5.1.2 Clearing

1. The clearing process will be based on the settlement statements in the Settlement Reports.
2. Each agency outside PAAC will settle with PAAC for Stored Value. If there has been excess revenue collected by the agency this revenue is owed to PAAC. If the agency has used excess fares the difference between fares used and revenues collected is owed by PAAC to the agency.
3. PAAC will issue invoice(s) and/or credits through their own financial system outside the AFC system.
4. Funds transfer takes place between PAAC and each RTA through their own financial system(s) outside the AFC system

5.1.3 Financial Audit

1. PAAC's and RTA's own financial systems will include all relevant information regarding auditing of the clearing process and funds transfer.
2. The settlement process will allow for financial auditing in such way that all transaction detail and summary reports used for settlement are to be stored in PDF files.

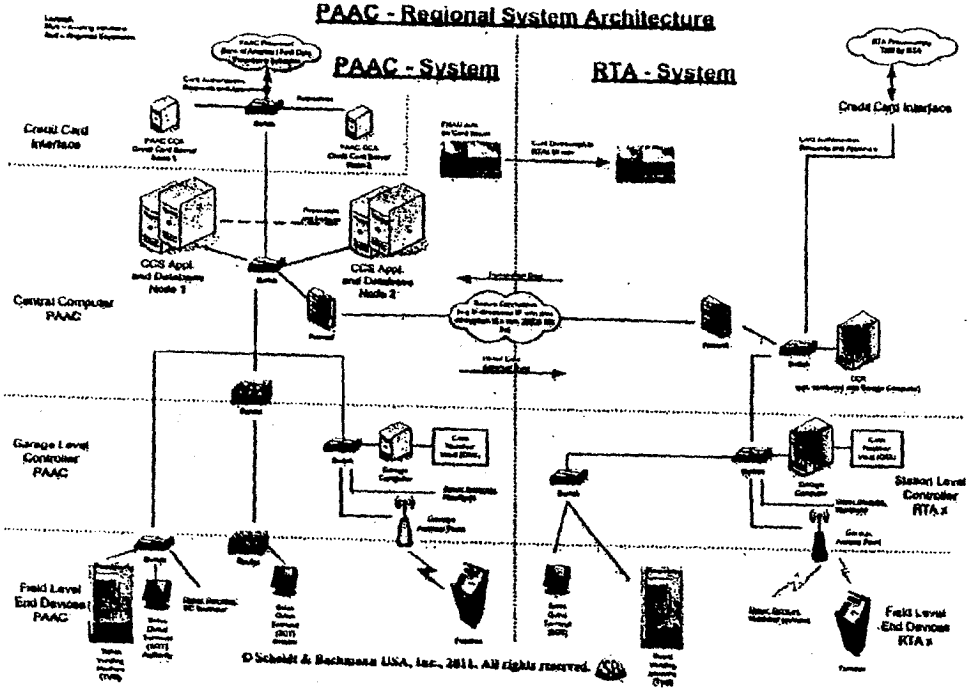


Figure 2- Regional System Architecture

PAAC – Data Exchange for Regional System

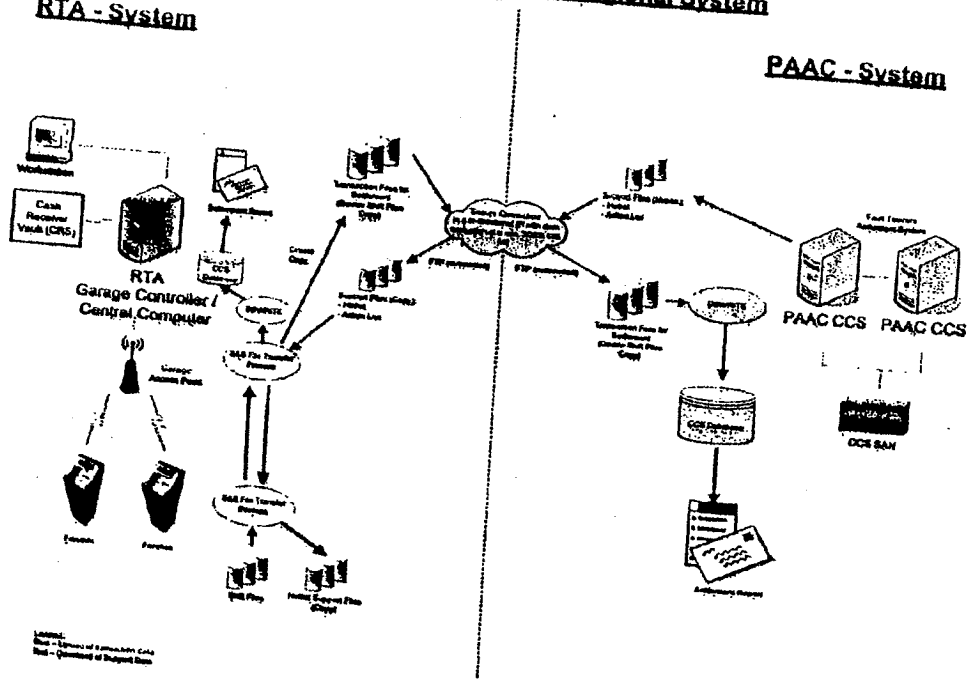


Figure 3- Exchange of Data

Revenue Settlement

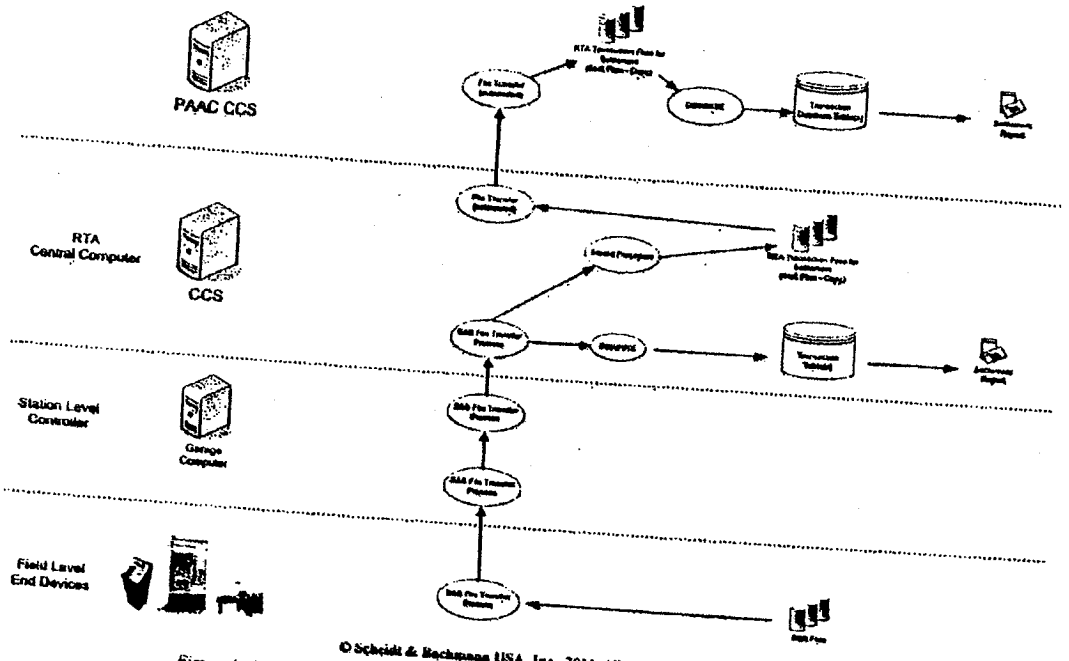


Figure 4 - Revenue Settlement Operation

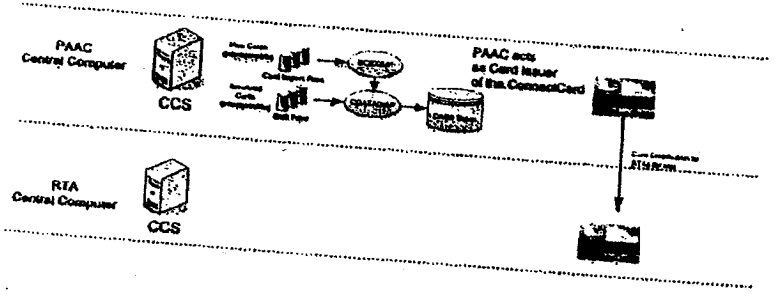


Figure 5 - Population of Card Inventory

6. Optional Solutions

Outside the Interoperability Concepts PAAC and the RTAs may pursue other solutions not required by the Agreement under Interoperability.

Note: Any of those optional solutions that combine fare media, fare products, operations of multiple agencies or similar solutions not explicitly required are considered as Out of Scope by S&B and would need to be discussed outside of the Agreement if interest by the agencies exists. Those solutions include but are not limited to:

- Issue of interoperable cards by agencies other than the Card Issuer (PAAC). Such solutions may require merging of card inventory data in PAAC's CCS and supplier coordination to establish unique smart card serial numbers.
- Use of PAACs credit card interface by RTAs. Depending on policies such solution may require to eliminate the RTA CCSs and connect the RTA station and garage level systems to the PAAC CCS and mange those from there.
- Shared sales of fare products, e.g. PAAC opts to sell fare products of participating RTAs through their Retail Terminals.
- Shared Web sites.

7. Attachments

#	Description	Reference
N/A		

8. Revision History

Revision	Description	Author	Date
1.0	Initial Release	B. Neuer	01/18/11
1.1	Update	B. Hoene	5/31/11
1.2	Update per PAAC-SB-528 and subsequent discussions with PAAC	B. Hoene	10/28/10 11/10/11
1.3	Update per PAAC-SB-624 and 2/9/12 meeting discussions with PAAC	B. Hoene	2/13/12

EXHIBIT B
TO
FARE SYSTEM INTEROPERABILITY AGREEMENT

Modules

System
- Log Off

Configuration
- Change Own Password

ConnectCard
- Card Management
- Individual Account Set-Up
- Anonymous Cards

Reports
- Reports (see Exhibit C)

Access to the above modules allow Regional Participants to:
- Register Smart Cards;
- Block a Smart Card;
- Check Stored Value Balance;
- Add to Stored Value;
- Change certain personal information for Smart Card Registration purposes
- Set up a Customer user account
- Set up a Customer Web User Account
- Review transactions for a particular Smart Card
- Change Authority CCS Password; and
- Run reports identified in Exhibit C.

EXHIBIT C
TO
FARE SYSTEM INTEROPERABILITY AGREEMENT

Reports

Report #	Report Description
2010	Transaction Details
2020	Usage Details
2030	Customer Service
2070	Action List Report
2080	User Action Log Report
2620	Detailed Sales Summary
2630	Ticket Summary
7070	Registered Smart Card Report
7080	Executed Smart Card Action
7090	Pending Smart Card Action
8000	Transaction Detail Summary
8010	Smart Card Settlement
8020	Sales Summary Smart Card Reconciliation
8030	Smart Card Total Reconciliation Report

EXHIBIT D
TO
FARE SYSTEM INTEROPERABILITY AGREEMENT

Restitution Procedure

EXHIBIT D
TO
FARE SYSTEM INTEROPERABILITY AGREEMENT

Restitution Procedures for Authority Customers

I. General

A. *Scope*

This document covers the Restitution Procedures for Authority Customers, but does not cover restitution, or the procedures related thereto, for Regional Customers.

B. *Purpose*

The purpose of the Restitution Procedures is to set forth guidelines for restitution by Authority for Authority Customers.

C. Definitions

In addition to the terms defined in the Agreement, the following terms are associated with these Restitution Procedures.

TERM	DEFINITION
Authority Customer Restitution	The process of replacing, for Authority Customers, lost registered Smart Cards or refunding or adjusting Stored Value and/or Authority Transit Products, whether due to a malfunction with the Authority CCS, a damaged Smart Card, or loss of a registered Smart Card.
Authority Customer Service Center	An Authority customer service center that handles inquiries from, and issues for, Authority Customers.
Authority Customer Service Agent	An Authority customer service representative who answers inquires and helps to resolve issues for Authority Customers.
Authority Customer Service Supervisor	An Authority customer service representative who manages Authority Customer Service Agents and resolves inquiries and issues for Authority Customers.

Smart Card Log	A form on which each Authority Service Center Agent records sales, restitutions, vouchers, refunds and revenue collected for his/her shift.
Smart Card Transaction Inquiry Form	A form completed by an Authority Customer or Authority Service Center Agent to request replacement of a lost registered Smart Card or refund or an adjustment in Stored Value or other Authority Transit Products for Authority Customers.

II. Process

1. The following process should be followed to initiate a claim or make an adjustment for Authority Customers. An Authority Customer should visit an Authority Customer Service Center or contact Authority Customer Service by telephone at 412-442-2000.

2. All Authority Customer restitutions will be handled by Authority Customer Service Agents and Authority Customer Service Supervisors. An Authority Customer Service Agent will complete a Smart Card Transaction Inquiry Form and submit the same to an Authority Customer Service Supervisor. The Authority Customer Service Supervisor will research the Smart Card account and read any notations made on the account.

3. The amount of Stored Value or other Authority Transit Products remaining on an Authority Customer's Smart Card will be determined using the Authority CCS, and a detailed report will be printed.

   (a) If an Authority Customer's Smart Card is not functioning (and is not lost or stolen), a new Smart Card will be issued with the remaining Stored Value or other Authority Transit Products determined to be due to such Authority Customer by the Authority Customer Service Center.

   (b) If an Authority Customer's registered Smart Card is lost or stolen, the remaining Stored Value or other Authority Transit Products determined to be due to such Authority Customer by the Authority Customer Service Center will be transferred onto a new Smart Card.

   (c) If an Authority Customer's Smart Card is not registered and the Smart Card is lost or stolen, the remaining Stored Value or other Transit Products will not be replaced or transferred.

4. Once an Authority Customer Service Supervisor has verified restitution, if any, is valid, as set forth above,then the Authority Customer Service Supervisor will complete the Smart Card Inquiry Form to indicate what, if any, Transit Products,

including Stored Value, were issued to an Authority Customer. If a Smart Card replacement is required, the necessary documentation will be delivered to the Authority Customer Service Center for replacement.

5. At the close of each business week, the Authority Customer Service Supervisor will calculate the total revenue and restitutions and record the information on the Smart Card Log. The Authority Customer Service Supervisor will then submit all supporting documentation to Authority's finance department.

If a Smart Card was purchased from a Regional Participant, or issues arise with the use of Stored Value or other Transit Products on a Regional Participant's transit system, the Customer should call that Regional Participant's customer service center and any adjustments required will be made by that office.

Authority reserves the right to amend, modify or replace this Restitution Procedure at any time.

APPENDIX 1
TO
FARE SYSTEM INTEROPERABILITY AGREEMENT

PAAC Corporate Information Security Policy

(See attached.)

PortAuthority
Connecting People to Life

Information Technology Policies

PAAC Corporate Information Security Policy

Policy #	IT-01	Effective Date	8/27/2012	Email	wbedenbaugh@portauthority.org
Version	1	Contact	Willie Bedenbaugh	Phone	412.237.7068

OVERVIEW 1
SCOPE 2
RESPONSIBILITIES 2
INFORMATION CLASSIFICATION AND HANDLING 3
INFORMATION ACCESS CONTROL 3
THIRD PARTY DATA HANDLING 5
PHYSICAL SECURITY 5
NETWORK SECURITY 7
INTERNET AND ELECTRONIC MAIL 8
ANTI-VIRUS AND SYSTEM SECURITY 9
USER RIGHTS AND EXPECTATIONS 10
POLICY MAINTENANCE 11
REFERENCES 12
RELATED DOCUMENTS 12
APPROVAL AND OWNERSHIP 12
REVISION HISTORY 12

OVERVIEW

Role Of Information And Information Systems – Port Authority of Allegheny County (PAAC) is critically dependent on information and information systems. If important information is disclosed to inappropriate persons, the company could suffer serious losses or legal ramifications. For example, if rider or client information is publicly disclosed, the organization's reputation could be harmed and litigation or fines could follow. For these and other important business reasons, executive management has initiated and continues to support an information security effort. One part of that effort is the definition of these information security policies.

Team Effort - To be effective, information security must be a team effort involving the participation and support of every PAAC employee who deals with information and information systems. In recognition of the need for teamwork, this policy statement clarifies the responsibilities of users and the steps they must take to help protect PAAC information and information systems. This document provides ways to prevent and respond to a variety of threats to information and information systems including unauthorized access, disclosure, duplication, modification, appropriation, destruction, loss, misuse, and denial of use.

SCOPE

Involved Persons - Every employee at PAAC must comply with the information security policies found in this and related information security documents. Employees who violate this and other information security policy statements may be subject to disciplinary action up to and including termination.

Involved Systems - This policy applies to all computer and network systems owned by or administered by PAAC. This policy applies to all operating systems, computers, and application systems. The policy primarily covers only information handled by computers and networks. Although this document includes mention of other manifestations of information such as voice and paper, for more information about the protection of information in paper form, see the Data Classification and Media Handling Policy IT-04.

RESPONSIBILITIES

Primary Departments Working On Information Security - Guidance, direction, and authority for information security activities are centralized for all PAAC organizational units in Information Technology Services. Information Technology Services is responsible for establishing and maintaining organization-wide information security policies, standards, guidelines, and procedures. Compliance checking and investigations to ensure that organizational units are operating in a manner consistent with these requirements is the responsibility of the Internal Audit Department and Information Technology Services. Disciplinary matters resulting from violations of information security requirements are handled by management working in conjunction with the Human Resources Division.

Three Categories Of Responsibilities - To coordinate a team effort, PAAC has established three categories, at least one of which applies to each employee. These categories are "Owner," "Custodian," and "User" as defined further herein. These categories define general responsibilities with respect to information security.

Owner Responsibilities - Information Owners are the Department managers, members of Senior Staff, or their delegates within PAAC who bear responsibility for the acquisition, development, and maintenance of production applications that process PAAC information. Production applications are computer programs that regularly provide reports in support of decision-making and other business activities. All production application system information must have a designated Owner. For each type of information, owners designate the relevant sensitivity classification, designate the appropriate level of criticality, define which users will be granted access, and approve requests for various ways in which the information may be utilized.

Custodian Responsibilities - Custodians are in physical or logical possession of either PAAC information or information that has been entrusted to the organization. Information Technology Services staff members clearly are the Custodians of system data. Whenever information is maintained only on a personal computer, the User is the Custodian of his/her data. Each type of production application system information must have one or more designated Custodians. Custodians are responsible for safeguarding the information, including implementing access control systems to prevent inappropriate disclosure, and backing up data so that critical

information will not be lost. Custodians are also required to implement, operate, and maintain the security measures defined by information Owners.

User Responsibilities - Users are responsible for familiarizing themselves with, and complying with, all PAAC policies, procedures, and standards dealing with information security. Questions about the appropriate handling of a specific type of information should be directed to either Information Technology Services or the Owner of the involved information.

INFORMATION CLASSIFICATION AND HANDLING

Consistent Information Handling - PAAC information, and information that has been entrusted to our organization, must be protected in a manner commensurate with its sensitivity and criticality. Security measures must be employed regardless of the media on which information is stored, the systems that process it, or the methods by which it is moved. Information must be protected in a manner that is consistent with its classification, no matter what its stage in the life cycle, from origin to destruction.

Information Classification Designations - PAAC has adopted an information classification system that categorizes information into 4 groupings. All information under PAAC control, whether generated internally or externally, falls into one of these categories: Confidential, For Internal Use Only and Public. All employees must familiarize themselves with the definitions for these categories and the steps that must be taken to protect the information falling into each of these categories. **Furthermore, no highly confidential personally identifiable information such as social security numbers or credit card data should be transmitted electronically or stored on any system without the explicit approval and controls of Information Technology Services.** Details can be found in the Data Classification and Media Handling Policy IT-04.

Information Classification Labeling - If information is confidential, from the time it is created until the time it is destroyed or declassified, it must be labeled with an appropriate information classification designation. Such markings must appear on all manifestations of the information. The vast majority of PAAC information falls into the "Private" or "Internal Use Only" category. For this reason, it is not necessary to apply a label to Internal Use Only information. Information without a label by default is classified as "For Internal Use Only. "

INFORMATION ACCESS CONTROL

Need to Know - Access to information in the possession of, or under the control of PAAC, must be provided based on the need to know. Information may only be disclosed to people who have a legitimate business need for the information. At the same time, employees must not withhold access to information when the Owner of the information instructs that it be shared. To implement the need-to-know concept, PAAC has adopted an access request and Owner approval process. Employees must not attempt to access sensitive information unless the relevant Owner has granted them access rights. When an employee changes job duties, including, but not limited to, termination, transfer, promotion and leave of absence, his or her supervisor must immediately notify Information Technology Services. The privileges granted to

all employees must be periodically reviewed by information Owners and Custodians to ensure that only those with a current need to know presently have access.

User IDs And Passwords - To implement the need-to-know process, PAAC requires that each employee accessing multi-user information systems have a unique user ID and a private password. These user IDs must be employed to restrict system privileges based on job duties, project responsibilities and other business activities. Each employee is personally responsible for the usage of his or her user ID and password. However, site-level employees are permitted to use a single dedicated User ID for the site to access certain informational systems.

Anonymous User IDs - With the exception of message boards, Internet sites, intranet sites, and other systems where all regular users are intended to be anonymous, users are prohibited from logging into any PAAC system or network anonymously. Anonymous access might, for example, involve use of "guest" user IDs. When users employ system commands that permit them to change active user IDs to gain certain privileges, they must have initially logged on with user IDs that clearly indicated their identities.

Difficult-to-Guess Passwords - Users must choose passwords that are difficult to guess. This means that passwords must not be related to one's job or personal life. For example, a car license plate number, a spouse's name, or fragments of an address must not be used. This also means passwords must not be a word found in the dictionary or some other part of speech. For example, proper names, places, technical terms, and slang must not be used.

Easily Remembered Passwords - Users can choose easily remembered passwords that are at the same time difficult for unauthorized parties to guess if they:

- string several words together
- shift a word up, down, left, or right one row on the keyboard
- bump characters in a word a certain number of letters up or down the alphabet
- combine punctuation or numbers with a regular word
- create acronyms from words in a song, poem, or another known sequence of words
- Deliberately misspell a word
- combine several preferences like hours of sleep desired and favorite colors.

Password Constraints - Passwords must be at least 7 characters long. Passwords must be changed every 90 days or at more frequent intervals. Passwords must contain a combination of at least one number or symbol. Whenever an employee suspects that a password has been compromised, that password must immediately be changed.

Password Storage - Passwords must not be stored in readable form in batch files, automatic logon scripts, software macros, terminal function keys, in computers without access control systems, or in other locations where unauthorized persons might discover them. Passwords must not be written down in some readily decipherable form and left in a place where unauthorized persons might discover them.

Sharing Passwords - If employees need to share computer-resident data, they must use electronic mail, databases, public directories on local area network servers, manual exchange, and other mechanisms. Although, user IDs can be shared for electronic mail and other informational purposes, the passwords must never be revealed to others. System administrators and other technical information systems staff are prohibited from asking an employee to reveal

their personal password. The only time a password should be known by another employee is when a temporary password is initially issued. These temporary passwords must then be changed the first time that the authorized user accesses the system. If a user believes that his or her user ID and password are being used by someone else, the user must immediately notify the information Owner. The only exemption to this rule will be for systems with limited security ramifications. For example, Intranet accounts and accounts used for specific internal applications.

Acceptable Use - All employees who wish to use PAAC multi-user computer systems must sign a compliance statement prior to being issued a user ID. A signature on this agreement indicates the involved user understands and agrees to adhere to PAAC policies and procedures related to computers and networks, including the instructions contained in this policy. The appropriate form is ITD-01.1 Acceptable Use Sign-off Sheet.

THIRD PARTY DATA HANDLING

Release Of Information To Third Parties - Unless it has specifically been designated as public, access to PAAC internal information by third parties is prohibited. Third parties may be given access to PAAC internal information only when a demonstrable need to know exists, when a PAAC non-disclosure agreement has been signed, and when such a disclosure has been expressly authorized by the relevant PAAC information Owner. If sensitive information is lost, disclosed to unauthorized parties, or is suspected of being lost or disclosed to unauthorized parties, the information Owner and Information Technology Services must be notified immediately.

Third-Party Requests For PAAC Information - Unless an employee has been authorized by the information Owner to make public disclosures, all requests for information about PAAC and its business must be referred to the Communications Officer and PAAC's Right to Know Officer. Such requests may include questionnaires, surveys, and newspaper interviews. This policy does not apply to sales and marketing information about PAAC products and services, nor does it pertain to customer technical support calls. If an employee is to receive sensitive information from third parties on behalf of the PAAC, this receipt must be preceded by the third-party signature on a PAAC release form.

External Disclosure Of Security Information - Information about security measures for PAAC computer and network systems is confidential and must not be released to people who are not authorized users of the involved systems unless approved by the Director of Information Technology. For example, publishing modem phone numbers, circuit ID numbers, Internet protocol addresses or other system access information in directories is prohibited. Public disclosure of electronic mail addresses is permissible.

PHYSICAL SECURITY

Physical Security to Control Information Access - Access to every location, datacenter, and other PAAC work area containing sensitive information must be physically restricted to those people with a need to know. When not in use, sensitive information must always be protected from unauthorized disclosure. When left in an unattended room, sensitive information in paper

form must be locked away in appropriate containers. During non-working hours, employees in areas containing sensitive information must store such information in a securely locked container. Unless information is in active use by authorized people, desks must be clear and clean during non-working hours to prevent unauthorized access to information. Employees must position their computer screens such that unauthorized people cannot look over their shoulder and see the sensitive information displayed.

Mobile Device Security - Mobile devices provide important functionality, allowing PAAC employees to have their computing resources at hand in meetings, those who travel on company business to be maximally functional and productive while away and those who occasionally work at home to eliminate duplication of resources, files, etc. Unfortunately, mobile devices that are lost as a result of theft or accident can leave the company at risk. The possible loss to the company could be substantial and includes losses in dollars, productivity and reputation. This policy addresses the actions that must be taken in order to minimize the risk of the theft of company owned mobile devices and the associated data belonging to the company. This policy applies to all PAAC employees, hereinafter referred to as "Custodians" who use a company owned mobile device. Each Custodian of a company-owned mobile device is responsible for the security of the device, regardless of whether the device is used in the office or away from the office. Special care should be taken in particularly vulnerable locations such as airports, conference centers, hotels and coffee shops. If it is inappropriate or impractical to secure a mobile device in a given situation, it is the Custodian's responsibility to take all reasonable steps to minimize the risk of loss of the device.

A mobile device is defined as any portable system that can store data. This includes but is not limited to the following devices.

- Laptop Computers
- Smartphones and Mobile phones (iPhone, Blackberry, Android based phones, etc..)
- Digital Tablets (iPad, Android, etc...)
- USB/Flash/Thumb drives, Memory Cards

Password-protect your mobile device – If your mobile device is lost or stolen, a device password may be all that stands in the way of someone reading your email and other sensitive data. Therefore, password protection on all corporate issued mobile devices is a requirement. Most devices employ password protection. For example, corporate issued laptops require a logon password and a Blackberry should be set with a lockout password. Remember, when selecting a password, the security of your system is only as strong as the password you select to protect it. You should have a complex password as noted above. PAAC will install and utilize mobile device management software on all corporate-issued devices to protect company information.

Theft Protection - All PAAC computer and network equipment must be physically secured if located in an open office. Local area network servers and other multi-user systems must be placed in locked cabinets, locked closets, or locked computer rooms. Computer and network gear may not be removed from PAAC offices unless the involved person has obtained proper authorization.

Reporting a Theft or Loss - If a Company-owned device is stolen or lost, its Custodian is expected to immediately notify Information Technology Services. Along with reporting the loss

of the equipment, the Custodian must report the loss of any data that may put the Company at risk.

NETWORK SECURITY

Internal Network Connections - All PAAC computers that store sensitive information and that are permanently or intermittently connected to internal computer networks must have a password-based access control system approved by Information Technology Services. Regardless of the network connections, all stand-alone computers handling sensitive information must also employ an approved password-based access control system. Users working with all other types of computers must employ the screen saver passwords that are provided with operating systems, so that after a period of "no activity," the screen will go blank until the correct password is re-entered. Multi-user systems throughout PAAC must employ automatic log off systems that automatically terminate a user's session after a defined period of inactivity.

External Network Connections - All in-bound session connections to PAAC computers from external networks must be protected with an approved password access control system. Users with personal computers connected to external networks are prohibited from leaving unattended modems turned-on while data communications software is enabled, unless an authorized dynamic password system has been previously installed. When using PAAC computers, PAAC employees must not establish connections with external networks including Internet service providers unless Information Technology Services has approved these connections.

Wireless Security - When connecting to wireless networks, at home or at other remote locations, it is the Custodian's responsibility to ensure that encryption is being used to protect the data that is being transmitted. Wi-Fi Protected Access (WPA or WPA2) is the most secure method of securing wireless data. Wired Equivalent Privacy (WEP) is an older and much less secure method of securing wireless data. WEP is still better than no encryption but it should be avoided if possible. Questions regarding wireless security should be directed to Information Technology Services.

Network Changes - With the exception of emergency situations, all changes to PAAC computer networks must be documented in a Change Control request, and approved in advance by Information Technology Services. Only persons who are authorized by Information Technology Services can make changes to PAAC networks. This process prevents unexpected changes from inadvertently leading to denial of service, unauthorized disclosure of information, and other problems. This process applies not only to employees but also to vendor personnel.

Mobile Computing and Telecommuting - At management's discretion, certain qualified employees may do some of their work at home. Permission to telecommute on a regular basis must be granted by each employee's immediate supervisor subject to the approval of the Division Director, Officer and/or Assistant General Manager based on a checklist of relevant factors. Continued permission to telecommute is partially dependent on continued compliance with a number of information security policies and standards. Periodic checking of electronic mail while on the road or from home is not considered telecommuting, but does require that employees follow many of the same security precautions.

Remote Access Security - PAAC provides remote access to employees with their supervisor's approval subject to the approval of the Division Director, Officer and/or Assistant General Manager. Additionally, vendors and contractors may be granted remote access to further PAAC business if they comply with access requirements and any additional restrictions deemed necessary by PAAC. Remote access will be granted under the following conditions. First, all users must comply with all the trusted access requirements, unless otherwise approved by Information Technology Services. Second, all users are responsible for ensuring that any computers that are connected to the PAAC networks are free of viruses or any other damaging software. Third, when remote access is no longer required, the user or supervisor will notify Information Technology Services within one business day in order to discontinue access. Information Technology Services will also perform periodic review of accounts for utilization. Finally, access control policies will be enforced and remotely accessible services will be limited to the minimum set required to support the business objectives of PAAC.

System Configuration Standards - All PAAC servers, hosts, firewalls, and other multi-user computers must be configured according to security requirements published by Information Technology Services.

INTERNET AND ELECTRONIC MAIL

Internet Access - Employees are provided with Internet access to perform their job duties, but this access may be terminated at any time at the discretion of management. Internet access is monitored and filtered to ensure that employees are not visiting sites unrelated to their jobs, and also to ensure that access is in compliance with PAAC policies. Employees may not make public representations on behalf of PAAC on Internet discussion groups and in other public forums, unless they have previously received authorization in writing from the Communications Officer to act in this capacity. All information received from the Internet should be considered to be suspect until confirmed by reliable sources. Employees must not place PAAC material on any publicly accessible computer system such as the Internet on behalf of PAAC unless both the information Owner and the Communications Officer have approved the posting. An approval process involving the Communications Department separately handles the establishment of Internet pages. **Users are prohibited from establishing any electronic commerce arrangements over Authority provided Internet unless Information Technology Services and the Communications Department have evaluated and approved of such arrangements.** Highly confidential and sensitive information, including passwords, social security numbers and credit card numbers, must not be sent across the Internet unless this information is in encrypted form.

Furthermore, PAAC has implemented strict content filtering for all locations with which Internet access is provided. Exemptions can be made to these controls with proper approval or for a justified business case.

Electronic Mail - PAAC employees who use computers in the course of their regular job duties can be granted an Internet electronic mail address and related privileges. All PAAC business communications sent by electronic mail must be sent and received using this company electronic mail address. See the PAAC Electronic Mail Policy IT-02 for more information.

ANTI-VIRUS AND SYSTEM SECURITY

Anti-Virus Software Installation
Virus screening software must be installed and enabled on all PAAC firewalls, FTP servers, mail servers, intranet servers, and desktop computers.

Virus Screening - All PAAC computer users must keep the current versions of approved virus screening software enabled on their computers. Users must not abort automatic software processes that update virus signatures. Virus screening software must be used to scan all software and data files coming from either third parties or other PAAC groups. This scanning must take place before new data files are opened and before new software is executed. Employees must not bypass or turn off the scanning processes that could prevent the transmission of computer viruses.

Virus Eradication - If employees suspect infection by a computer virus, they must immediately stop using the involved computer and call the Information Technology Services Helpdesk at 7444 or 412-237-7444. USB drives and other magnetic storage media used with the infected computer must not be used with any other computer until the virus has been successfully eradicated. The infected computer must also be immediately isolated from internal networks. Users must not attempt to eradicate viruses themselves. Qualified Information Technology Services staff must complete this task in a manner that minimizes both data destruction and system downtime.

Clean Backups - All disk-based computer software must be copied prior to its initial usage, and such copies must be stored in a secure location such as a software repository or locked file cabinet. These master copies must not be used for ordinary business activities, but must be reserved for recovery from computer virus infections, hard disk crashes, and other computer problems.

Software Sources - PAAC computers and networks must not run software that comes from sources other than other PAAC Departments, well-known systems security authorities, or established computer, network, or commercial software vendors. Software downloaded from electronic bulletin boards, shareware, public domain software, and other software from untrusted sources must not be used unless it has been subjected to a rigorous testing regimen approved by Information Technology Services.

Written Specifications for Owners - All software developed by in-house staff, intended to process critical or sensitive PAAC information, must have a formal written specification. This specification must include discussion of security risks and controls including access control systems and contingency plans. The specification must be part of an agreement between the information Owner and the system developer. Macros in spreadsheets and word processing documents are not considered software in this paragraph.

Security Sign-Off Required - Before being used for production processing, new or substantially changed application systems must have received approval from Information Technology Services for the controls to be employed. This requirement applies to desktop computers just as it does to larger systems.

Formal Change Control - All computer and communications systems used for production processing must employ a documented change control process that is used to ensure that only

authorized changes are made. This change control procedure must be used for all significant changes to production system software, hardware, communications links, and procedures. This policy applies to personal computers running production systems and larger multi-user systems.

Systems Development Procedures - All production software development and software maintenance activities performed by in-house staff must adhere to Information Technology policies, standards, procedures, and other systems development procedures. These procedures include the proper testing, training, and documentation of developed systems

Adequate Licenses - PAAC management must coordinate through Information Technology Services to make appropriate arrangements with software vendors for additional licensed copies, if and when additional copies are needed for business activities. All software must be purchased and installed through Information Technology Services.

Unauthorized Copying - Users must not copy software provided by PAAC to any storage media, transfer such software to another computer, or disclose such software to outside parties without advance permission from their Information Technology Services. Ordinary backup copies are an authorized exception to this policy.

Backup Responsibility – Information Technology Services is the Custodian for all PAAC system data backups. All backups containing critical or sensitive information must be stored at an approved off-site location with either physical access controls or encryption. A contingency plan must be prepared for all applications that handle critical production information. It is the responsibility of the information Owner to ensure that this plan is adequately developed, regularly updated, and periodically tested.

User Rights and Expectations

Rights To Material Developed - While performing services for PAAC, PAAC has exclusive rights to patents, copyrights, inventions, or other intellectual property originated or developed by employees. All programs and documentation generated by, or provided by employees for the benefit of PAAC are the property of PAAC. PAAC asserts the legal ownership of the contents of all information systems under its control. PAAC reserves the right to access and use this information at its discretion.

Right To Search And Monitor - PAAC is responsible for operating, maintaining, and protecting its electronic communications networks and ensuring compliance with PAAC's policies. To accomplish these objectives, PAAC may monitor and search at any time all PAAC information systems. By making use of PAAC systems, users consent to permit all information they create, access, send, receive or store on PAAC systems to be monitored, searched, reviewed, and disclosed at the discretion of PAAC management. Monitoring, searches, reviews, and disclosure will be done only for legitimate, business purposes. Monitoring, searches and reviews will be done in a reasonable manner aimed at collecting information that is relevant to the legitimate, business purpose. This includes personal information accessed, created, sent or received while using PAAC computers, devices, networks, and systems. The information systems subject to such examination include, but are not limited to, electronic mail system files, personal computer hard drive files, "I" drives, voice mail files, printer spool files, fax machine output, desk drawers, and storage areas. All searches of this nature must be conducted after the approval of the Legal Department. Because PAAC computers and networks are provided for

business purposes only, employees have no expectation of privacy associated with their use of these information systems. PAAC management retains the right to remove from its information systems any material it views as offensive or potentially illegal.

Personal Use - PAAC information systems are intended to be used for business purposes only. Incidental personal use is permissible if the use does not consume more than a trivial amount of resources that could otherwise be used for business purposes, does not interfere with employee productivity and does not preempt any business activity. Permissible incidental use of an electronic mail system would, for example, involve sending a message to schedule a luncheon. Use of PAAC information systems for chain letters, non-PAAC sponsored charitable fund raising campaigns, political campaign or advocacy efforts, religious efforts, private business activities, or personal amusement and entertainment is prohibited without prior management authorization.

Unbecoming Conduct - PAAC management reserves the right to revoke the system privileges of any user at any time. Conduct that interferes with the normal and proper operation of PAAC information systems, which adversely affects the ability of others to use these information systems, or that is harmful, vulgar, obscene, threatening, intimidating, harassing, or a violation of PAAC's policies against discrimination, harassment, on the basis of age, race, religion, sex, ethnicity, nationality, disability, or other protected class, status, or characteristic is not permitted.

Security Compromise Tools - Unless specifically authorized in writing by Information Technology Services and General Counsel, PAAC employees must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise information systems security. Examples of such tools include those that defeat software copy protection, discover secret passwords, identify security vulnerabilities, or decrypt encrypted files. Without this type of approval, employees are prohibited from using any hardware or software that monitors the traffic on a network or the activity on a computer.

Prohibited Activities - Users must not test, or attempt to compromise computer or communication system security measures unless specifically approved in advance and in writing by the Director of Information Technology. Incidents involving unapproved system hacking, password guessing, file decryption, bootleg software copying, or similar unauthorized attempts to compromise security measures may be unlawful, and will be considered serious violations of PAAC internal policy. Short-cuts bypassing systems security measures, and pranks and practical jokes involving the compromise of systems security measures are absolutely prohibited.

Mandatory Reporting - All suspected policy violations, system intrusions, virus infestations, and other conditions that might jeopardize PAAC information or PAAC information systems must be immediately reported to Information Technology Services.

POLICY MAINTENANCE

Initial approval of all IT related policies will be made at the Authority Senior Staff level. All IT related policies and all PAAC Security Documentation will be maintained by Internal Audit and Information Technology Services. These policies will be reviewed annually and approved by the Director of Information Technology and/or an approved Authority representative.

Modification - This policy may be modified only in writing and must be approved by the Director

or Information Technology and no other employee has the authority to modify this policy.

REFERENCES

This section reserved for future use.

RELATED DOCUMENTS

This section reserved for future use.

APPROVAL AND OWNERSHIP

Created By	Title	Date
Willie Bedenbaugh	Director of IT	8/8/2012
Approved By	**Title**	**Date**
Authority Senior Staff		8/23/2012

REVISION HISTORY

Version	Revision Date	Review Date	Description
1.0	8/23/2012	8/27/2012	Initial Posting
1.0		8/12/2013	Yearly review/WPB

APPENDIX 2
TO
FARE SYSTEM INTEROPERABILITY AGREEMENT

PAAC Internet Acceptable Use Policy

(See attached.)

PortAuthority
Connecting People to Life

Information Technology Policies

PAAC Internet Acceptable Use Policy

Policy #	IT-03	Effective Date	8/27/2012	Email	wbedenbaugh@portauthority.org
Version	1	Contact	Willie Bedenbaugh	Phone	412.237.7068

Objectives and Scope 1
Approval for Use 1
Information Integrity 2
Information Confidentiality 3
Public Representations 3
Copyrighted Materials 4
Access Control 4
Personal Use 5
Privacy Exceptions 6
Reporting Security Problems 6
References 7
Related Documents 7
Approval and Ownership 7
Revision History 7

OBJECTIVES AND SCOPE

Opportunities and Risks - The wide array of resources, services, and inter-connectivity available through the Internet all introduce new business opportunities, and new security and privacy risks. In response to the risks, this policy describes the Port Authority of Allegheny County's (PAAC) official policy regarding Internet security.

Applicability - This policy applies to all users, employees, contractors, consultants, temporaries, and volunteers, who use the Internet with PAAC computing or networking resources. Within this policy, the term "Internet" is used to reference all electronic communications which access the internet, including but not limited to, web sites, Internet relay chat (IRC), message boards, or blogs. The policy applies to all those who use the Internet and represent themselves as being connected in some way with PAAC. All of these Internet users are expected to be familiar with and fully comply with this policy. Questions about the policy should be directed to management or Information Technology Services. Violations of this policy can lead to revocation of system privileges. . In addition, employees who violate this and other information security policies may be subject to disciplinary action up to and including discharge.

APPROVAL FOR USE

Prior Management Approval - PAAC users must not access the internet without a proper understanding of the associated personal and business risks. Access to the Internet, aside from electronic mail, will be provided to only those users who have a legitimate business need for

such access. An employee's access to the Internet is at the discretion of each employee's supervisor. The ability to access the Internet and engage in other Internet activities is not a fringe benefit to which all users are entitled. If a user does not have sufficient Internet access, but needs access for a particular project, he or she can use special shared systems established by PAAC management.

INFORMATION INTEGRITY

Information Reliability - All information acquired from the Internet must be considered suspect until confirmed by separate information from another source. Before using free Internet-supplied information for business decision-making purposes, users must corroborate the information by consulting other sources.

Virus Checking - All non-text files downloaded from non-PAAC sources through the Internet must be screened with current virus detection software prior to being used. Whenever an external provider of the software is not trusted, downloaded software must be tested by Information Technology Services on a stand-alone, non-production machine. The use of digital signatures to verify that a file has not been altered by unauthorized parties is recommended, although this does not assure freedom from viruses, Trojan horses, and other problems.

Software Downloading - PAAC has implemented an automatic software distribution system to install the latest release of licensed software as required on PAAC computers. A separate system is used to automatically trace all software residing on these same systems. As discussed in IT-07 PAAC Computer Security Policy, users must not install software on their PAAC-supplied computers, whether the software was downloaded from the Internet or procured elsewhere.

Push Technology - Automatic updating of software or information on PAAC computers through background push Internet technology is prohibited unless the involved vendor's system has been tested and approved by Information Technology Services.

Spoofing Users - Before users release any internal PAAC information, enter into any contracts, or order any products through public networks, the identity of the individuals and organizations contacted must be confirmed. Identity confirmation is ideally performed through digital signatures or digital certificates. In cases where these certifications are not available, users should contact Information Technology Services for assistance.

User Anonymity - Misrepresenting, obscuring, suppressing, or replacing a user's identity on the Internet or any PAAC electronic communications system is forbidden. The user name, electronic mail address, organizational affiliation, and related information included with messages or postings must reflect the actual originator of the messages or postings. Use of anonymous FTP logons, anonymous UUCP logons, HTTP or web browsing, and other access methods established with the expectation that users would be anonymous are strictly prohibited.

Electronic Mail Attachments - Users must not open electronic mail attachments unless the user is familiar with the sender and the attachments were expected. When they are expected from a known and trusted sender, attachments must be scanned with a virus package prior to being opened.

Responding to Information Requests - Users must never respond to unsolicited requests for personal information, including passwords or credit card numbers from an electronic mail

message. Any such message should be immediately reported to Information Technology Services.

Web Page Changes - Users must not establish new Internet pages on behalf of PAAC, or make modifications to existing web pages dealing with PAAC business, unless they have obtained the approval of the Communications Officer. Modifications include the addition of links to other sites, updating the information displayed, and altering the graphic layout of a page. All posted material must have a consistent and polished appearance, be aligned with business goals and protected with adequate security measures.

Web Page Archives - Every version of the PAAC Internet site and commerce site files must be securely archived. The Director of Information Technology will designate a web master who will keep this archive and provide copies of historical pages on demand.

INFORMATION CONFIDENTIALITY

Information Exchange - PAAC software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-PAAC party for any purposes other than business purposes expressly authorized by management. Exchanges of software or data between PAAC and any third party must not proceed unless a written agreement, approved by the PAAC Legal Department, has been signed.

Posting Materials -Users must not post unencrypted PAAC material on any publicly-accessible Internet computer that supports anonymous FTP or similar publicly-accessible services, unless the posting of these materials has been approved by the Communications Officer. PAAC internal information must not be placed in any computer unless the persons who have access to that computer have a legitimate business need to know the involved information.

Message Interception - PAAC confidential, proprietary, or private information must not be sent over the Internet unless it has been encrypted by approved methods. Unless specifically known to be in the public domain, source code must always be encrypted before being sent over the Internet.

Security Parameters - Unless a connection is known to be encrypted, credit card numbers, telephone calling card numbers, fixed logon passwords, and other security parameters designed to be used to gain access to goods or services, must not be sent over the Internet in readable form. Encryption processes are permissible if they are approved by Information Technology Services.

PUBLIC REPRESENTATIONS

External Representations - Employees must take special care to ensure that they do not represent PAAC on Internet discussion groups and in other public forums, unless they have previously received authorization in writing from the Communications Officer to act in this capacity. With the exception of ordinary marketing and customer service activities, all representations on behalf of PAAC must be cleared by the Communications Officer.

PAAC Email Addresses - Users posting information on any publicly available web site must not include their PAAC email address. PAAC issues separate email addresses for specific public postings. Users who require the external posting of their PAAC email address must request permission from their management or the Communications Officer.

Appropriate Behavior - Whenever any affiliation with PAAC is included with an Internet message or posting, PAAC users are advised that written attacks by the user are strictly prohibited. Messages or posts containing information that is harassing, intimidating, threatening, disruptive, offensive to others, or harmful to morale or otherwise violates PAAC's policies against discrimination or harassment, on the basis of age, race, religion, sex, ethnicity, nationality, disability, or other protected class, status, or characteristic are prohibited.

Removal Of Postings - Those messages sent to Internet discussion groups, electronic bulletin boards, or other public forums, that impliedly or explicitly indicate that they were made on behalf of PAAC, must be removed if they contain information that is vulgar, obscene, threatening, intimidating, harassing, or a violation of PAAC's policies against discrimination or harassment, on the basis of age, race, religion, sex, ethnicity, nationality, disability, or other protected class, status, or characteristic are prohibited. The decision to remove messages must be made by the Communications Officer. Depending on the circumstances, individuals responsible for the message will be informed of the decision and given the opportunity to remove the message themselves.

Disclosing Internal Information - Users must not publicly disclose confidential internal PAAC information through the Internet that may adversely affect the PAAC customer relations or public image unless the approval of the Communications Officer has been obtained. Such information includes but is not limited to business prospects, projects now in the planning stage, system performance analyses and internal information systems problems.

Inadvertent Disclosure - Care must be taken to properly structure comments and questions posted to mailing lists, public news groups, Usenet, and related public postings on the Internet. Before posting any material, users must consider whether the posting could put PAAC at a significant disadvantage or whether the material could cause public relations problems. Users should bear in mind that several separate pieces of information can be pieced together by outside sources to form a picture revealing confidential information that could be used against PAAC. Users must never post on the Internet the specific computer or network products employed by PAAC.

COPYRIGHTED MATERIAL

Copyrights - When at work, or when PAAC computing or networking resources are employed, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden. The reproduction, forwarding, or in any other way republishing or redistribution of words, graphics, or other copyrighted materials must be done only with the permission of the author or Owner. Users must assume that all materials on the Internet are copyrighted unless specific notice states otherwise. When information from the Internet is integrated into internal reports or used for other purposes, all material must include labels such as "copyright, all rights reserved" and specifics about the source of the information.

ACCESS CONTROL

Inbound User Authentication - All users wishing to establish a real-time connection with PAAC internal computers through the Internet must employ a product approved by Information Technology Services. These products also must authenticate remote users at a firewall before permitting access to the PAAC internal network. This authentication process must be achieved through a system approved by Information Technology Services.

Remote Machine Security - Users who have not installed required software patches or upgrades, or whose systems are virus-infested will be disconnected from the PAAC network until they have reestablished a secure computing environment. Remote users are responsible for insuring their machines are up-to-date with the latest applicable software releases and utilization of anti-virus software.

Restriction Of Third-Party Access - Inbound Internet access privileges must not be granted to third-party vendors, contractors, consultants, temporaries, outsourcing organization personnel or other third parties unless the relevant system manager determines that these individuals have a legitimate business need for such access. These privileges must be enabled only for specific individuals and only for the time period required to accomplish approved tasks.

Data Aggregators - Users must not provide their Internet user IDs and passwords to data aggregators, data summarization and formatting services, or any other third parties.

Internet Service Providers - With the exception of field and mobile computer users, users must not employ Internet service provider accounts and dial-up lines to access the Internet with PAAC computers. All Internet activity must pass through PAAC firewalls so that access controls and related security mechanisms can be applied. Users must employ their PAAC electronic mail address for Internet electronic mail. Use of a personal electronic mail address for this purpose is prohibited.

Establishing Network Connections - Unless the prior approval of Information Technology Services has been obtained, users must not establish Internet or other external network connections that could permit non-PAAC users to gain access to PAAC systems and information. These connections include the establishment of multi-computer file systems, Internet pages, Internet commerce systems, and FTP servers.

Establishing New Business Channels - Unless the Communications Officer, General Counsel and the Director of Information Technology have approved in advance, users must not use new or existing Internet connections to establish new business channels. These channels include electronic data interchange arrangements, electronic malls with online shopping, and online database services.

Conducting Business Over The Internet - Unless advance approval of the Purchasing Department has been obtained, PAAC Users must not purchase any goods or services related to daily business operations utilizing PAAC funds from Internet sources.

PERSONAL USE

Personal Use - PAAC information systems are intended to be used for business purposes only. Incidental personal use is permissible if the use does not consume more than a trivial amount of resources that could otherwise be used for business purposes, does not interfere with employee productivity and does not preempt any business activity. Permissible incidental use of an electronic mail system would, for example, involve sending a message to schedule a luncheon. PAAC electronic communication systems must not be used for non-PAAC sponsored charitable fund raising campaigns, political campaign or advocacy efforts, religious efforts, private business activities, or personal amusement and entertainment. In certain instances and with prior management authorization, PAAC electronic communication systems may be utilized for non-PAAC sponsored charitable fund raising or community relations events when it is deemed,

in management's sole discretion, that the proposed fund raising or community relations event would reflect positively on PAAC as an organization and integral part of the community that it serves.

Offensive Web Sites - PAAC accepts no responsibility for the content that users may encounter when they use the Internet. When and if users make a connection with web sites containing objectionable content, they must promptly move to another site or terminate their session. Users using PAAC computers who discover they have connected with a web site that contains sexually explicit, racist, sexist, violent, or other potentially offensive material must immediately disconnect from that site.

Blocking Sites and Content Types - The ability to connect with a specific web site does not in itself imply that users of PAAC systems are permitted to visit that site. PAAC may, at its discretion, restrict or block the downloading of certain file types that are likely to cause network service degradation. These file types include graphic and music files.

Use of "social networking" sites - Users are prohibited from using PAAC systems to access web sites designed for the sole purpose of posting and sharing personal information. Exceptions require the approval of the employee's Director and must be requested through the IT Helpdesk. PAAC reserves the right to block access to these or other web sites.

PRIVACY EXCEPTIONS

No Default Protection - Users using PAAC information systems or the Internet must realize that their communications are not automatically protected from viewing by third parties. Unless encryption is used, Users must not send information over the Internet if they consider it to be confidential or private.

Management Review - At any time and without prior notice, PAAC management reserves the right to examine electronic mail messages, files on personal computers, web browser cache files, web browser bookmarks, logs of web sites visited, computer system configurations, and other information stored on or passing through PAAC computers.

Logging - PAAC routinely logs the web sites visited, files downloaded, time spent on the Internet, and related information. Department managers can receive reports of such information and use it to determine what types of Internet usage are appropriate for their department's business activities.

Junk Electronic Mail - Users must not use PAAC computer systems for the transmission of unsolicited bulk electronic mail advertisements or commercial messages that are likely to trigger complaints from the recipients. These prohibited messages include a wide variety of unsolicited promotions and solicitations such as chain letters, pyramid schemes, and direct marketing pitches. When users receive unwanted and unsolicited electronic mail, they must refrain from responding directly to the sender. They must forward the message to the IT Helpdesk and Information Technology Services will then take steps to prevent further transmissions.

REPORTING SECURITY PROBLEMS

Notification Process - If sensitive PAAC information is lost, disclosed to unauthorized parties, or suspected of either, the Director of Information Technology must be notified immediately. If any unauthorized use of PAAC information systems has or is suspected of taking place, the

Director of Information Technology must be notified immediately. Whenever passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed, the Director of Information Technology must be notified immediately. All unusual systems behavior, such as missing files, frequent system crashes, and misrouted messages must be immediately reported to the IT Helpdesk. The specifics of security problems must not be discussed widely but should instead be shared on a need-to-know basis.

False Security Reports - Users in receipt of information about system vulnerabilities must forward it to the Director of Information Technology, who then will determine what if any action is appropriate. Users must not personally redistribute system vulnerability information to other users.

Testing Controls - Users must not test or probe security mechanisms at either PAAC or other Internet sites unless they have obtained written permission from the Director of Information Technology. The possession or the usage of tools for detecting information system vulnerabilities, or tools for compromising information security mechanisms, are prohibited without the advance permission of the Director of Information Technology.

Modification - This policy may be modified only in writing and must be approved by the Director or Information Technology and no other employee has the authority to modify this policy.

REFERENCES

Reserved for Future Use.

RELATED DOCUMENTS

Reserved for Future Use.

APPROVAL AND OWNERSHIP

Created By	Title	Date
Willie Bedenbaugh	Director of IT	8/8/2012
Approved By	**Title**	**Date**
Authority Senior Staff		8/23/2012

REVISION HISTORY

Version	Revision Date	Review Date	Description
1.0	8/23/2012	8/27/2012	Initial Posting
1.0		8/14/2013	Yearly review/WPB

APPENDIX 3
TO
FARE SYSTEM INTEROPERABILITY AGREEMENT

PAAC Firewall Policy

(See attached.)

PortAuthority
Connecting People to Life

Information Technology Policies

PAAC Firewall Policy

Policy #	IT-05	Effective Date	8/27/2012	Email	wbedenbaugh@portauthority.org
Version	1	Contact	Willie Bedenbaugh	Phone	412.237.7068

Policy Objectives 1
Scope and Applicability 1
Specific Requirements 2
References 5
Related Documents 5
Approval and Ownership 5
Revision History 5

POLICY OBJECTIVES

Firewalls are an essential component of the Port Authority of Allegheny County (PAAC) information systems security infrastructure. Firewalls are defined as security systems that control and restrict network connectivity and network services. Firewalls establish a control point where access controls may be enforced. Connectivity defines which computer systems are permitted to exchange information. A service is sometimes called an application, and it refers to the way for information to flow through a firewall. Examples of services include file transfer protocol (FTP) and web browsing (HTTP). This policy defines the essential rules regarding the management and maintenance of firewalls at the PAAC and it applies to all firewalls owned, rented, leased, or otherwise controlled by PAAC users.

SCOPE AND APPLICABILITY

Policy Applicability - All firewalls on PAAC networks, whether managed by employees or by third parties, must follow this policy. Departures from this policy will be permitted only if approved in advance and in writing by the Director of Information Technology. Employees who violate this and other information security policies may be subject to disciplinary action up to and including discharge.

Playing The Role Of Firewalls - In some instances, systems such as routers, air gaps, telecommunications front ends, or gateways may be functioning as though they are firewalls when they are not formally known as firewalls. All PAAC systems playing the role of firewalls, whether they are formally called firewalls, must be managed according to the rules defined in this policy. In some instances this will require that these systems be upgraded so that they support the minimum functionality defined in this policy.

SPECIFIC REQUIREMENTS

Required Documentation - Prior to the deployment of every PAAC firewall, a diagram of permissible paths with a justification for each, and a description of permissible services accompanied by a justification for each, must be submitted to the Director of Information Technology. Permission to enable such ports and services will be granted by the Director of Information Technology only when these paths or services are necessary for important business reasons, and sufficient security measures will be consistently employed. The conformance of actual firewall deployments to the documentation provided will be periodically checked by authorized Authority employees. The acceptable paths (ACL), ports, and services documentation must be reviewed at least every 6 months.

Physical Network diagrams are also necessary to display all connections to and from secured networks. Network diagrams will be reviewed at least every quarter by the Manager of Data Center Operations and/or authorized Authority employees.

Default Denial - Every connectivity path and service that is not specifically permitted by this policy and supporting documents issued by Information Technology Services must be blocked by PAAC firewalls. The list of currently approved ports and services must be documented and distributed to all system administrators with a need to know by Information Technology Services. An inventory of all access paths into and out of the PAAC internal networks must be maintained by Information Technology Services.

Specifically, any traffic from the Scheidt & Bachmann environment to and from external or unsecured internal networks will require explicit authorization and will be properly documented.

Regular Testing - Because firewalls provide such an important control measure for PAAC networks, their strength and proper configuration must be tested on a regular basis. Where vendor software supports it, this testing must include the use of configuration management software that automatically checks to determine whether firewalls remain configured and running in a manner that is consistent with PAAC security policies. This testing process must include consideration of defined configuration parameters, enabled services, permitted connectivity paths, current administrative practices, and adequacy of the deployed security measures. These tests must include the quarterly execution of vulnerability identification and the annual performance of penetration tests. These tests must be performed by technically proficient persons in a dedicated Information Security role or through 3rd Parties. Those responsible for either the administration or management of the involved firewalls must not perform these tests.

Logs - All changes to firewall configuration parameters, enabled services, and permitted connectivity paths must be logged. All suspicious activity that might be an indication of either unauthorized usage or an attempt to compromise security measures also must be logged. The integrity of these logs must be protected with checksums, digital signatures, encryption, or similar measures.

Intrusion Detection - All PAAC firewalls must be combined with intrusion detection systems approved by Information Technology Services. Among other potential problems, these intrusion detection systems must detect unauthorized modifications to firewall system files, and detect denial of service attacks in progress. Such intrusion detection systems must also notify the proper technical staff in a position to take corrective action.

Contingency Planning and Incident Response - Technical staff working on firewalls must prepare and obtain Information Technology Services approval for contingency plans that address the actions to be taken in the event of various problems including system compromise, system malfunction, system crash, system overload, and Internet service provider unavailability. These contingency plans must be kept current to reflect changes in the PAAC information systems environment. These plans must be periodically tested to ensure that they will be effective in restoring a secure and reliable networking environment.

External Connections - All in-bound real-time Internet connections to the PAAC secured networks must pass through a firewall. No PAAC computer system may be attached to the Internet unless it is protected by a firewall. The computer systems requiring firewall protection include web servers, electronic commerce servers, and mail servers. All laptops/Mobile systems must employ a Host-based firewall approved by Information Technology Services. Wherever a firewall supports it, logon screens must have a notice indicating that the system may be accessed only by authorized users and users who log on represent they are authorized to do so. The notice must also indicate that unauthorized system usage or abuse is subject to disciplinary action up to and including discharge and may be referred to the proper authorities for criminal prosecution, and system usage will be monitored and logged.

Extended User Authentication - Inbound traffic to support firewalls and systems in the Scheidt & Bachmann environment must in all instances involve extended or 2 factor user authentication measures approved by Information Technology Services. Examples of approved extended user authentication systems include tokens, dynamic passwords and digital certificates.

Encryption - To prevent unauthorized disclosure of sensitive and valuable information, all inbound traffic, with the exception of Internet mail and informative websites that access PAAC networks must be encrypted with the products approved by Information Technology Services. These connections are often SSL based or virtual private networks (VPNs). The VPNs permissible on PAAC networks combine extended user authentication functionality with communications encryption functionality

Firewall Access Mechanisms - All PAAC firewalls must have unique passwords or other access control mechanisms. The same password or access control code must not be used on more than one firewall. Whenever supported by the involved firewall vendor, those who administer PAAC firewalls must have their identity validated through extended user authentication mechanisms.

Passwords must meet the requirements set forth in IT-07 PAAC Computer Security Policy.

Firewall Access Privileges - Privileges to modify the functionality, connectivity, and services supported by firewalls are restricted to those individuals so designated by the Director of Information Technology, with a business need for these same privileges. All firewalls must have at least two staff members who are adequately trained to make changes, as circumstances require. One of these firewall administration staff members shall be readily available at all times.

Secured Subnets - Portions of the PAAC internal network that contain sensitive or valuable information, such as the computers used by the Scheidt & Bachmann systems and all wireless networks, must employ a secured subnet. Access to this and other subnets must be restricted with firewalls and other access control measures. Based on periodic risk assessments,

Information Technology Services will define the secured subnets required in the Information Security Architecture.

Demilitarized Zones - All Internet commerce servers including payment servers, database servers, and web servers must be protected by firewalls, and be located within a demilitarized zone (DMZ), a subnet that is protected from the Internet by one or more firewalls. An internal network, such as an intranet, is also protected from the DMZ subnet by one or more firewalls.

Network Management Systems - Firewalls must be configured so that they are visible to internal network management systems. Firewalls also must be configured so that they permit the use of auditing tools to be used by authorized PAAC staff members.

Firewalls must be configured for access to approved Time-synchronization servers in order to keep system time accurate.

Disclosure Of Internal Network Information - The internal system addresses, configurations, products deployed, and related system design information for PAAC networked computer systems must be restricted such that both systems and users outside the PAAC internal network cannot access this information. Proper use of Network and Port Address Translation (NAT, PAT) and other similar technologies is required on all PAAC firewalls.

Secure Backup - Current offline back-up copies of firewall configuration files, connectivity permission files, firewall systems administration procedural documentation files, and related files must be stored at all times. A permissible alternative to offline copies involves online secure or encrypted versions of these same files. Where system software permits an automatic backup strategy is preferred. Otherwise, a manual procedure to securely backup all firewall configurations will be implemented. This procedure will need to be performed after all configuration changes.

Virus Screening and Content Screening - Virus screening software approved by Information Technology Services must be installed and enabled on all PAAC firewalls or through dedicated proxy systems. Because the files passing through a firewall may be encrypted or compressed, firewall-based virus detection systems may not detect all virus-infected files. For this reason, virus-screening software is also required at all PAAC servers and mobile/desktop computers. Both content screening software and software that blocks users from accessing certain non-business web sites must also be enabled on all PAAC firewalls or through dedicated proxy systems.

Firewall Dedicated Functionality – Perimeter firewalls must run on dedicated machines that perform only security functions, i.e... IDS, Anti-virus gateway, and content filtering. Firewalls must have only the bare minimum operating systems software resident and enabled on them. Where the supporting operating system permits it, all unnecessary and unused systems software must be removed from firewalls.

Firewall Change Control – Information Technology Services must review and approve all changes to firewall configurations, excluding vendor-provided upgrades, patches and fixes. Major changes to the PAAC internal networking environment, any changes to the production business applications supported, and any major information security incident must trigger an additional and immediate review of the firewall policy. The changes should be documented with proper rollback procedures.

Updates - PAAC firewalls must be running the latest release of software to repel attacks. Where available from the involved vendor, all PAAC firewalls must subscribe to software maintenance and software update services. Staff members responsible for managing firewalls must install and run these updates within 30 business days of issue.

Monitoring Vulnerabilities – PAAC staff members responsible for managing firewalls must subscribe to relevant sources providing current information about firewall vulnerabilities. Any vulnerability that appears to affect PAAC networks and systems must promptly be brought to the attention of Information Technology Services.

Firewall Physical Security - All PAAC firewalls must be located in locked rooms accessible only to those who perform authorized firewall management and maintenance tasks approved by Information Technology Services management. The placement of firewalls in an open area within a general purpose data processing center is prohibited, although placement within separately locked rooms or areas, which themselves are within a general data processing center is acceptable.

Modification - This policy may be modified only in writing and must be approved by the Director or Information Technology and no other employee has the authority to modify this policy.

REFERENCES

Reserved for Future Use.

RELATED DOCUMENTS

Reserved for Future Use.

APPROVAL AND OWNERSHIP

Created By	Title	Date
Willie Bedenbaugh	Director of IT	8/8/2012
Approved By	**Title**	**Date**
Authority Senior Staff		8/23/2012

REVISION HISTORY

Version	Revision Date	Review Date	Description
1.0	8/23/2012	8/27/2012	Initial Posting
1.0		8/15/2013	Yearly review/WPB

APPENDIX 4
TO
FARE SYSTEM INTEROPERABILITY AGREEMENT

PAAC Computer Security Policy

(See attached.)

PortAuthority
Connecting People to Life

Information Technology Policies

PAAC Computer Security Policy

Policy #	IT-07	Effective Date	8/27/2012	Email	wbedenbaugh@portauthority.org
Version	1	Contact	Willie Bedenbaugh	Phone	412-237-7068

Objectives and Scope 1
Business Use Only 1
Configuration Control 2
Access Control 2
Viruses 3
Backups, "I" Drives and Software Purchases 3
Destruction 4
Documentation 4
Networking 5
Physical Security 5
Rights and System Security 6
References 7
Related Documents 7
Approval and Ownership 7
Revision History 7

Objectives and Scope

A large portion of Port Authority of Allegheny County (PAAC) business is conducted with computers, including Macintoshes, UNIX workstations, portable computers, handheld computers, digital assistants, and similar equipment dedicated to a single user's activity. Protection of computers and the information handled by these systems is an essential part of doing business at PAAC. To this end, this policy provides information security instructions applicable to all employees who use PAAC computers. All computer users are expected to comply with this policy as a condition of continued employment. This policy applies whether computers are standalone or connected to a network such as a local area network, intranet or internet. Employees who violate this and other information security policies may be subject to disciplinary action up to and including discharge.

Business Use Only

Business Use Only - In general, PAAC computer and communication systems are intended to be used for business purposes only. Incidental use is nonetheless permissible if the use does not consume more than a trivial amount of resources that could otherwise be used for business purposes, does not interfere with worker productivity, does not preempt any business activity, and does not cause distress, legal problems, or morale problems for other employees. PAAC prohibits the use of its systems in ways that are harassing, intimidating, threatening, disruptive, offensive to others, or harmful to morale or otherwise violate PAAC's policies against

discrimination or harassment, on the basis of age, race, religion, sex, ethnicity, nationality, disability, or other protected class, status, or characteristic .

CONFIGURATION CONTROL

Changes To Application Software - PAAC has a standard list of permissible software that users can run on PAAC computers. Employees must not install any other software on computers without obtaining advance permission from Information Technology Services. Employees must not permit automatic software installation routines to be run on PAAC computers unless these routines have been approved by Information Technology Services. Unless separate arrangements are made with Information Technology Services, upgrades to authorized software will be downloaded to PAAC computers automatically. Unapproved software may be removed without advance notice to the involved worker.

Changes To Operating System Configurations - On PAAC computer hardware, employees must not change operating system configurations, upgrade existing operating systems, or install new operating systems. If such changes are required, they must be performed by Information Technology Services personnel.

Changes To Hardware - Computer equipment supplied by PAAC must not be altered or added to in any way without the prior knowledge of and authorization from Information Technology Services.

ACCESS CONTROL

Access Control Package - All PAAC computers must run an access control package approved by Information Technology Services. Typically these packages require a fixed password at the time a computer is booted and again after a certain period of inactivity. Information Technology Services will set the time frame for this period of inactivity, at which point the contents of the screen are obscured, to 15 minutes or less. If sensitive information resides on a computer, the screen must immediately be protected with this access control package, or the device turned off, whenever a worker leaves the location where the computer is in use.

Choice Of Passwords - The user-chosen passwords employed by access control software packages, and the keys employed by encryption packages, must be at least 7 characters in length. These passwords and keys must be difficult to guess. Words in a dictionary, derivatives of user IDs, and common character sequences such as "123456" must not be employed. Details such as spouse's name, license plate, social security number, and birthday must not be used unless accompanied by additional unrelated characters. User-chosen passwords and keys must not be any part of speech including, proper names, geographical locations, common acronyms and slang.

Storage Of Passwords - Employees must maintain exclusive control of their passwords. They must not share them with others at any time. Passwords must not be stored in readable form in batch files, automatic logon scripts, software macros, terminal function keys, in computers without access controls or in any other locations where unauthorized persons might discover them.

Encryption Of Confidential Information - All computerized Confidential information must be encrypted when not in active use, for example, when not manipulated by software or viewed by an authorized user. The use of physical security measures such as safes, locking furniture, and locking office doors is recommended as a supplementary measure to protect confidential information.

Logging Of Events Related To Confidential Information - Computers handling Confidential information must securely log all significant computer security relevant events. Examples of computer security relevant events include password guessing attempts, attempts to use privileges that have not been authorized, modifications to production application software, and modifications to system software.

VIRUSES

Virus Program Installed - All computers must continuously run the current version of antivirus software approved by Information Technology Services. The current version of this antivirus software must be automatically downloaded to each computer when the device is connected to the PAAC internal network. Employees must not abort this download process. At a minimum, this package must execute whenever external storage media is supplied.

Decompression Before Checking - Externally-supplied thumb drives, CD-ROMs, and other removable storage media must not be used unless they have been checked for viruses. Attachments to electronic mail must not be executed or opened unless they have been checked for viruses. Externally-supplied, computer-readable files, software programs, databases, word processing documents, and spreadsheets must be decompressed prior to being subjected to an approved virus-checking process. If the files have been encrypted, they must be decrypted before running a virus-checking program.

Eradicating Viruses - Employees must not attempt to eradicate a virus without Information Technology Services assistance. If employees suspect infection by a virus, they must immediately stop using the involved computer, physically disconnect from all networks, and call the Information Technology Help Desk at 412-237-7444 (7444 from a PAAC phone). If the suspected virus appears to be damaging information or software, employees must immediately turn off the computer.

Intentional Introduction of Viruses - Users must not intentionally write, compile, copy, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any PAAC computer system. Users who do so may be subject to discipline, up to and including discharge. Further, users may be subject to criminal prosecution for such activity.

BACKUPS, "I" DRIVES AND SOFTWARE PURCHASES

Archival Copies - All computer software that is not standard PAAC software must be copied prior to its initial usage, and such copies must be stored in a safe and secure location. These master copies, perhaps the media issued by the vendor, must not be used for ordinary business activities, but must be reserved for recovery from virus infections, hard disk crashes, and other computer problems. Documentation about the licenses for such software must be retained to get technical support, qualify for upgrade discounts and verify the legal validity of the licenses.

Periodic Backup - All sensitive, valuable or critical information resident on PAAC technology systems must be periodically backed up. Such backup processes must be performed at least daily. Selected files from backups must be periodically restored to demonstrate the effectiveness of the backup process.

"I" Drives – All PAAC computer users should user their "I" drive for storage of work related documents. Documents stored on the "I" drive are periodically archived by Information Technology Services. No documents should be stored on a computer's "C" drive or on a user's desktop.

Software Purchases – No software should be purchased for any PAAC computer or network related equipment without the prior approval of Information Technology Services. All software must be checked for compatibility in PAAC network environment before any approval for purchase is given.

Copyright Protection - Making unauthorized copies of licensed and copyrighted software, even if for "evaluation" purposes, is forbidden. PAAC permits reproduction of copyrighted materials only to the extent legally considered fair use or with the permission of the author or Owner. If employees have any questions about the relevance of copyright laws, they must contact PAAC Legal counsel. Unless they receive information to the contrary, employees must assume that software and other materials are copyrighted.

DESTRUCTION

Deletion of Old Information - Employees must delete information from their computers if it is clearly no longer needed or potentially useful. Prior to deleting any PAAC information, employees should consult the related Document Retention Schedule. Use of an erase feature is not sufficient for sensitive information because the information may be recoverable. Sensitive information should be deleted by an overwrite program approved by Information Technology Services.

Destruction Of Information - Prior to disposal, defective or damaged media containing sensitive information must be destroyed using methods approved by Information Technology Services. All hardcopy containing sensitive Information must be disposed of in approved shredding bins or through a cross-cut paper shredder.

DOCUMENTATION

Documentation For Production Systems - Every user who develops or implements software or hardware to be used for PAAC production business activities must document the system in advance of its deployment. The documentation must be written so that the system may be run by persons unacquainted with it. Such documentation must be prepared even when standard software, such as a spreadsheet program, is employed.

Contingency Plans - When a computer is used as a critical part of any production business application, it must have a documented and tested contingency plan. Contingency plans must be prepared in accordance with the guidelines issued by Information Technology Services.

Consistent Classification Marking - If information is sensitive, from the time when it is created until it is destroyed or declassified, it must be labeled with an appropriate data classification designation. Such markings must appear on hardcopy versions of the information, and the labels for storage media containing this information. Further information about data classification and marking can be found in IT-04 PAAC Data Classification and Media Handling Policy.

NETWORKING

Modems – Wireless or wired modems inside or attached to PAAC computers are not permitted. PAAC mobile laptop computers are an exception to this rule but must be approved by Information Technology Services. When in PAAC facilities, users needing to make outbound connections with remote servers or the Internet must route their connections through the Network Access Control (NAC) systems. Information Technology Services controls access to this system.

Internet - As a matter of policy, inbound Internet connections to PAAC computers is forbidden unless these connections employ a system approved by Information Technology Services. These systems must employ both user authentication features with at least fixed passwords and data interception prevention features, such as encryption.

Downloading Sensitive Information - Sensitive PAAC information may be downloaded from a multi-user system to a computer only if a clear business need exists, adequate controls to protect the information are currently installed on the involved computer, and advance permission from the information Owner has been obtained. This policy is not intended to cover electronic mail or memos, but does apply to databases, master files, and other information stored on servers and other multi-user devices. This applies regardless of the media on which information is stored, the locations where the information is stored, the systems technology used to process the information, the people who handle it, or the processes by which information is handled.

Installation Of Communications Lines - Employees and vendors must not make arrangements for, or actually complete the installation of voice or data lines with any carrier if they have not obtained approval from Information Technology Services.

Establishing Networks - Employees must not establish electronic bulletin boards, local area networks, modem connections to existing internal networks, Internet commerce systems, or other multi-user systems for communicating information without the specific approval of Information Technology Services.

Automatic Device Synchronization - Systems that automatically exchange data between devices, such as a digital assistant and a computer, must not be enabled unless the systems have been evaluated and approved by Information Technology Services.

PHYSICAL SECURITY

Equipment Theft - All computer equipment with a minimum intrinsic value must be tagged with identification information that clearly indicates it is PAAC property. Information Technology Services will keep records of the tags and locations of the equipment. Unless considered a high

theft risk, the minimum value for tagged equipment is $500.00. All desktop PCs, laptops and digital tablets will be tagged and tracked.

Donation Or Sale Of Equipment - Before computer equipment or storage media that has been used for PAAC business is provided to any third party, the equipment or media must be physically inspected by Information Technology Services to determine that all sensitive information has been removed.

Lending Computers To Others - Employees must never lend a PAAC computer to another person or organization without the approval of Information Technology Services.

Custodians Of Equipment - The primary user of a computer is considered a Custodian of the equipment. If the equipment has been damaged, lost, stolen, borrowed, or is otherwise unavailable for normal business activities, a Custodian must promptly inform their department manager. With the exception of portable equipment (i.e. laptops), computer equipment must not be moved or relocated without the knowledge and approval of Information Technology Services.

Use Of Equipment - Employees must not bring their own computers, computer peripherals, or computer software into PAAC facilities without prior authorization from their department head. Employees must not use their own computers for production PAAC business unless these systems have been evaluated and approved by Information Technology Services. Writing memos or reports is not considered production PAAC business for purposes of this policy.

Property Removal Approval - Computers, portable computers, and related information systems equipment must not leave PAAC offices unless approved by PAAC management. Equipment owned by employees and brought into PAAC offices also must have PAAC management approval.

Positioning Display Screens - The display screens for all computers used to handle sensitive or valuable data must be positioned such that the information cannot be readily viewed through a window, by persons walking in a hallway, or by persons waiting in reception and related areas. Care must also be taken to position keyboards so that unauthorized persons cannot readily see employees enter passwords, encryption keys, and other security-related parameters.

Locking Sensitive Information - When not being used by authorized employees, or when not clearly visible in an area where authorized persons are working, all hardcopy sensitive information must be locked in file cabinets, desks, safes, or other furniture. When not being used, or when not in a clearly visible and attended area, all computer storage media containing sensitive information must be locked in similar enclosures.

Environmental Considerations – Servers, computers and any associated network equipment running production applications must also have uninterruptible power systems approved by Information Technology Services.

RIGHTS AND SYSTEM SECURITY

Rights To Programs Developed - Without a specific written exception, all computer programs and documentation generated by, or provided to employees for the benefit of PAAC are the property of PAAC. All other material developed by PAAC employees using computers is considered the property of PAAC, including patents, copyrights, and trademarks.

Browsing - Employees must not browse through PAAC computer systems or networks. Steps taken by employees to legitimately locate information needed to perform their job are not considered browsing. Use of the PAAC intranet is not considered browsing.

Tools To Compromise Systems Security - Unless specifically authorized by Information Technology Services, PAAC employees must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise PAAC information systems security. Examples of such tools include those that defeat software copy protection, discover secret passwords, identify security vulnerabilities, or decrypt encrypted files.

Reporting Problems - Users must promptly report all information security alerts, warnings, and suspected vulnerabilities to the Information Technology Help Desk. Users must not use PAAC systems to forward such information to other users, whether the other users are internal or external to PAAC.

Modification - This policy may be modified only in writing and must be approved by the Director or Information Technology and no other employee has the authority to modify this policy.

REFERENCES

Reserved for Future Use.

RELATED DOCUMENTS

Reserved for Future Use.

APPROVAL AND OWNERSHIP

Created By	Title	Date
Willie Bedenbaugh	Director of IT	8/8/2012
Approved By	**Title**	**Date**
Authority Senior Staff		8/23/2012

REVISION HISTORY

Version	Revision Date	Review Date	Description
1.0	8/23/2012	8/27/2012	Initial Posting
1.0		8/16/2013	Yearly review/WPB

APPENDIX 5
TO
FARE SYSTEM INTEROPERABILITY AGREEMENT

PAAC Third Party Service Provider Policy

(See attached.)

PortAuthority
Connecting People to Life

Information Technology Services Policies

PAAC Third Party Service Provider Policy

Policy #	IT-08	Effective Date	8/27/2012	Email	wbedenbaugh@portauthority.org
Version	1	Contact	Willie Bedenbaugh	Phone	412-237-7068

Overview and Scope 1
Third Party Verification List 1
Requirements for Third Party 1
References 3
Related Documents 3
Approval and Ownership 3
Revisions 3

Overview and Scope

This policy is designed to ensure that proprietary Port Authority of Allegheny County (PAAC) information is not disclosed to a third party that is not able to properly protect the information. The third party will be required to sign a "non-disclosure" agreement. The third party will also be required to provide an "information security policy" that is acceptable to Information Technology Services. Information Technology Services will determine if the third party has a system of internal controls that can realistically be expected to adequately protect PAAC proprietary information. If Information Technology Services is not satisfied with the security policy document, then the request for proprietary information will be denied. For third parties that are government agencies, the word "proprietary" may be replaced with a more acceptable term. This policy is intended for third-party organizations rather than individuals. However, if an individual is being considered for the receipt of proprietary information, PAAC will prepare an Agreement that will set forth a list of minimum security measures that the third party individual must agree to in writing.

Employees who violate this and other information security policies may be subject to disciplinary action up to and including discharge.

Third Party Verification List

Third Party Vendor List – Information Technology Services will maintain a list of approved vendors verified under the "Third Party Service Providers Policy". At a minimum, this list will be updated annually or as required by vendor additions and removals.

Requirements for Third Party

Third-Party Security Policy - Before any proprietary PAAC information is disclosed to a third party, this third party must sign a PAAC non-disclosure agreement and submit a copy of its

information security policy for approval by PAAC Information Technology Services. The third party information security policy must be resubmitted and recertified annually.

Third-Party Access Terms And Conditions - Before any third party is given access to internal PAAC IT systems, an Agreement defining the terms and conditions of such access must have been signed by an officer of the third-party organization and is subject to the approval of PAAC's Information Technology Services and Legal Departments.

Security Measures At Third-Party Organizations for Remote Access - Before a user ID for remote access can be issued to a third party, documentary evidence of an information security system or process must be provided to, and approved by, PAAC Information Technology Services. The third party must agree in writing to maintain this system or process to prevent unauthorized and improper use of PAAC systems

Sending of Information to Third Party - Prior to sending any Confidential or For Internal Use Only Information to a third party for copying, printing, formatting, or other handling, the third party must sign a PAAC non-disclosure agreement.

Information Handling At Contract Termination - If PAAC terminates its contract with any third-party organization that is handling PAAC private information, this same third-party organization must immediately thereafter destroy or return all of the PAAC private data in its possession. Evidence of the third party's compliance to this policy will be submitted in writing to PAAC.

Outsourced data destruction must use approved methods - PAAC must verify the data specific methods of all third parties contracted for destruction of equipment containing sensitive data.

Approval for 3rd Party Removal of Any Equipment - Before PAAC equipment with an initial purchase value of $5000.00 or above is sold, disposed of, recycled, donated, or otherwise conveyed to a third party, the written approval of the Accounting Department must first be obtained.

Unannounced Repair Visits - Every third party Information Technology-related repair person or maintenance person who appears at PAAC facilities without being called by an Information Technology Services employee must be denied access to the facilities. All such incidents must be promptly reported to Information Technology Services. Those that have been called by an employee must have their requested presence confirmed by a guard, receptionist or authorized employee before they are given access to the facilities.

Third Party Service Providers Work During Office Hours - All third party IT service providers (including maintenance, repair, construction, and information systems) must do their in-person work on PAAC premises during regular PAAC business hours. Exceptions will be made only if an Information Technology Services manager's approval is obtained in advance and if these users are continuously escorted while on PAAC premises.

Modification - This policy may be modified only in writing and must be approved by the Director or Information Technology and no other employee has the authority to modify this policy.

REFERENCES

Reserved for Future Use.

RELATED DOCUMENTS

ITD-4.1 PAAC Non-Disclosure Agreement

APPROVAL AND OWNERSHIP

Created By	Title	Date
Willie Bedenbaugh	Director of IT	8/8/2012
Approved By	**Title**	**Date**
Authority Senior Staff		8/23/2012

REVISION HISTORY

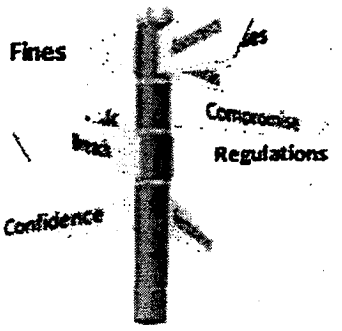
Version	Revision Date	Review Date	Description
1.0	8/23/2012	8/27/2012	Initial Posting
1.0		8/16/2013	Yearly review/WPB

2.7.10 PCI Compliance Requirement

Proposer shall provide evidence of PCI compliance with associations as well as evidence of PCI compliance and SAS 70 Type II reports, or its equivalent for outsourced functions to third parties. Proposer shall indicate in its proposal if its standard agreement acknowledges that the processor is responsible for all account holder data.

Due to the highly confidential nature of the SOC1 Report and its potential to compromise our security measures, we do not provide this report without execution of our NDA. We are happy to provide the report upon execution of our NDA.

Bank of America Merchant Services and all subcontractors and third-party processors (if any) are compliant with applicable Card Organization rules, including those related to PCI DSS. Because the Bank of America Merchant Services' legal entity does not directly process, store, or transmit card data, we are not required to possess a PCI DSS Report on Compliance. However, our equity owner, First Data, specifically our affiliate First Data Merchant Services Corporation (FDMS), is required to be PCI DSS compliant and is certified as such.



Trustwave confirms PCI compliance annually for FDMS. FDMS is Bank of America Merchant Services' service provider for the card processing services described in this RFP. Trustwave is FDMS' Qualified Security Assessor. To verify PCI DSS compliance for the purposes of this RFP response, Authority may refer to the publicly available Global List of PCI DSS Validated Service Providers at http://www.visa.com/splisting

We have also attached a letter confirming PCI compliance as issued to FDMS by Trustwave. Refer to Attachment 2.7.

Trustwave®
Smart security on demand

trustwave.com

December 10, 2013

John Hellickson
Vice President Enterprise Security, Risk, and Compliance (ESRC)
First Data Merchant Services (FDMS-Payspring)
6200 S Quebec St., Ste 2000 W
Greenwood Village, CO 80111

First Data Merchant Services (FDMS-Payspring) engaged Trustwave to conduct an assessment to determine whether First Data Merchant Services (FDMS-Payspring) has satisfactorily met the Payment Card Industry Data Security Standard (PCI-DSS) version 2.0. Trustwave is a PCI SSC certified Quality Security Assessor.

The following business units and platforms were in scope for this assessment:

First Data Merchant Services (FDMS-Payspring)
North and South Platforms

Based upon the information provided by First Data Merchant Services (FDMS-Payspring) regarding policies, procedures and technical systems that store, process or transmit cardholder data, an onsite assessment, and a vulnerability scan of these systems, Trustwave has determined that First Data Merchant Services (FDMS-Payspring) has satisfactorily met the applicable PCI DSS requirements as of September 13, 2013.

As of the date of this letter, First Data Merchant Services (FDMS-Payspring) remains enrolled in Trustwave's PCI DSS assessment program and will have external vulnerability scans performed on certain First Data Merchant Services (FDMS-Payspring) systems to help detect commonly known vulnerabilities during the term of our agreement with First Data Merchant Services (FDMS-Payspring). One of the requirements to maintain compliance is to successfully pass periodic vulnerability scans of these systems. In addition, you must also continually identify and provide to Trustwave information regarding any new system that stores, processes or transmits cardholder data, so that those systems can also be scanned.

If you have any questions concerning this matter, please do not hesitate to contact me at Compliance-QA@trustwave.com. Thank you.

Sincerely,

Digitally signed by Todd Skipper
DN: cn=Todd Skipper, o=QA, ou=Trustwave, email=tskipper@trustwave.com, c=US
Date: 2013.12.10 12:41:15 -06'00'

Todd Skipper
Acting Director of Quality Management

CORPORATE HEADQUARTERS
70 West Madison Street
Suite 1050
Chicago, IL 60602
Tel: +1 (312) 873 7500

EMEA HEADQUARTERS
Westminster Tower
3 Albert Embankment
London, SE1 7SP
Tel: +44 (0) 845 456 9611

ASIA-PACIFIC HEADQUARTERS
Level 2, 46 Hunter Street
Sydney NSW 2000
Australia
Tel: +61 (0) 2 9236 4200

LATIN AMERICA HEADQUARTERS
Rua Cincinato Braga, 340 nº 71 - Edifício Delta Plaza
Bairro Bela Vista - São Paulo - SP
CEP: 01333-010 – BRASIL
Tel: +55 (11) 4064 6101

Privacy Policy

Thank you for visiting the TriMet website at trimet.org (the "Site") and reviewing our privacy policy. This privacy policy is effective as of December 27, 2006, and applies only to the Site. It is designed to assist you in understanding how we collect and use the personal information you provide to us, and to assist you in making informed decisions when using our Site. TriMet respects the privacy of your personal information.

This privacy policy covers the following areas:

- what information we collect through our Site;
- how we use the information;
- with whom we may share the information;
- what choices you have about our collection, use and disclosure of the information;
- what security procedures are in place to protect the loss, misuse or alteration of information under our control; and
- how you can correct any inaccuracies in your information.

1. Information collection

TriMet collects information on the Site at two different stages. First, we use server logs to collect anonymous, aggregate information (such as browser type, ISP, IP address, referring/exit pages, platform type, date/time stamp, number of clicks) from all visitors to the Site. Our Site also uses a standard technology called "cookies" to collect information about how the Site is used. Information gathered through cookies may include the pages viewed and the amount of time spent at the Site. This type of information is typically not linked to any personally identifiable information and is used primarily in the aggregate to generate statistical reports about the use of our Site. TriMet does reserve the right to connect information collected through its server logs with other personally identifiable information.

Second, we require certain information when you use services available on the Site. For example, when you contact us by email, we may collect your email address and any other personal information you provide. When you subscribe to one of our electronic newsletters, you must provide your name and a valid email address. You may also provide your address, telephone number and organizational affiliation, and you may choose to create a password

for managing your account. If you purchase items from the online store, TriMet and its payment processing partner will collect additional information necessary for payment and delivery. If you apply for employment through the Site, we will collect personal information such as your name, address and other employment-related information.

To unsubscribe from any of our email lists, simply click on the link labeled "Change your account settings" at the bottom of any email from us, or contact us at subscriptions@trimet.org.

2. Personal information of children under 13

TriMet complies with the requirements of the Childrens Online Privacy Protection Act (COPPA) and the FTC's Rule interpreting COPPA (16 CFR § 512). The Site is not directed to children, and we do not knowingly collect any personally identifiable information on the Site from children under 13 years of age.

3. Use of your personal information

TriMet does not sell, rent or disclose personally identifiable information to any third party not affiliated with us, except for disclosure to service providers who may assist us in such areas as data storage, and in accordance with Paragraph 4 below. However, users should be aware that TriMet is a public agency and personal information provided to TriMet may be subject to disclosure in accordance with public records laws. Information in anonymous, aggregated form may be shared freely. TriMet will not use your personal information to send you unsolicited commercial offers. However, we may need to contact you for certain purposes, as for example in response to your inquiry, or with a message regarding the status of the Site.

4. Disclosure of personal information as required by law

We will disclose personal information when required by law, or if we have a good-faith belief that such action is necessary to (a) comply with a current judicial proceeding, a court order or legal process served on us, (b) protect and defend our rights, or (c) protect the rights, property, and other interests of our users or others.

5. Links

The Site contains links to other sites. TriMet is not responsible for the privacy practices or

content of these other sites. We encourage you to be aware when you leave our Site and to read the privacy statements and terms/conditions of use for each and every site that collects personally identifiable information. This privacy statement applies solely to information collected by the TriMet Site.

6. Security

We take reasonable precautions to protect your information. For example, we encrypt certain communications through our Site with 128-bit encryption, the industry standard for strong encryption. However, given the nature of the Internet and the fact that network security measures are not infallible, we cannot guarantee the security of your information.

If you have any questions about the security at our Site, you can send a message to the webmaster at webadmin@trimet.org.

7. Correcting, updating, deleting and deactivating personal information

If your information changes, you may contact us to correct, update or delete and deactivate our records.

8. Notification of changes

TriMet may modify the terms of this privacy policy at any time by updating this posting. If this privacy policy changes materially so that we are going to use your personally identifiable information in a manner different from that stated at the time of collection, or if we make any material changes in our privacy practices that affect customer information already stored in our database, we will prominently post a notice on the main page and other pages to alert you about the change. You should check the Site periodically to remain informed of the latest version of the privacy policy.

9. Contact information

webadmin@trimet.org

Terms of Use

Welcome to the Tri-County Metropolitan Transportation District of Oregon ("TriMet") website (the "Service" or "Site"). By continuing use of the Service or accessing any materials on the Site, you agree to these Terms of Use ("Terms"), as they may be updated or modified by TriMet at any time in its discretion. If you do not agree to them, do not use the Site or download any material from it.

1. Linking policy—not a public forum

The Site is not a forum for public communication and debate, but a means for TriMet to provide information relating to TriMet services, programs, objectives, missions and projects to the public and its customers. All decisions as to the placement of links to external sites or pages from the Site will be made by TriMet in its sole discretion. TriMet is not responsible for and does not endorse the content of any third party website. Third party websites are accessed at your own risk. TriMet permits links from other web sites in accordance with the following conditions:

- The appearance, position and other aspects of the link may not be such as to damage or dilute the goodwill associated with TriMet's name and trademarks or be displayed in any manner that is likely to cause confusion among the public or disparage or discredit TriMet;
- The appearance, position and other attributes of the link may not create the false impression that an organization or entity is sponsored by, affiliated with or associated with TriMet or that views expressed on the website are those of TriMet. TriMet reserves the right to require that the linking website include notice stating that it is an unofficial web site and is not endorsed by, sponsored by or affiliated with TriMet and that any views expressed on the website are not those of TriMet; and
- When selected by a user, the link must display the Site full-screen and not within a frame on the linking website.

2. RSS feeds

RSS feeds are part of the Service and your use of the RSS feeds is subject to all of these Terms. Any reference in these Terms to the content of the Site includes the content of the RSS Feeds. In addition, the following conditions apply. You may not alter the text, links or other content of the RSS feeds in any way. If your site displays the content of the RSS feeds,

you must use a platform that permits all links contained in the RSS feeds to function as intended by TriMet. You may not insert any "splash page" or any other content between a link in a TriMet RSS feed and the linked-to TriMet page.

3. No guaranteed availability

TriMet reserves the right at any time and from time to time to modify or discontinue the Service (or any part thereof), temporarily or permanently, with or without notice to you. You agree that TriMet will not be liable to you for any modification, suspension or discontinuance of the Service.

4. Termination of service to you

You agree that TriMet, in its sole discretion, may terminate your password, account (or any part thereof) or use of the Service, and remove and discard any content within the Service, for any reason, including, without limitation, our belief that you have violated or acted inconsistently with the letter or spirit of these Terms. You agree that any termination of your access to the Service under any provision of these Terms may occur without prior notice to you, and you also agree that TriMet will not be liable to you for any termination of your access to the Service.

5. Restrictions on use

All materials published on the Site, including, but not limited to, trademarks, service marks, maps, schedules, arrival information, fare information, photographs and illustrations (collectively, the "Content"), is the property of TriMet unless otherwise indicated. Third-party trademarks are the property of their respective owners. You may use the Content displayed on the Site for personal, non-commercial use only, provided that you do not remove any trademarks, copyright or any other notice contained in such content. Developer use of TriMet's real-time arrival data requires registration and is governed by separate terms. Any other use, including reproduction, modification, distribution, transmission, republication, display or performance, is strictly prohibited without the express written consent of TriMet.

6. Copyrights and trademarks

All Content of this Site including content of the RSS feeds is the property of TriMet or its content suppliers, and is protected by United States and international copyright laws. The compilation of the Content on this Site is the exclusive property of TriMet, and is likewise

protected by US and international copyright laws.

All trademarks, service marks and trade names ("Trademarks") of TriMet used herein or in the RSS feeds (including, but not limited to, TRIMET, MAX, WES, TRANSITTRACKER and QUICK DROP, the slogan "SEE WHERE IT TAKES YOU" and the TriMet logos (see below)) are trademarks or registered trademarks of TriMet and may not be used in any manner that is likely to cause confusion, or in any manner that disparages or discredits TriMet. The TriMet trademarks may not be used in connection with the products or services of others, except for the use of a text link or a TriMet web logo to link to this site, in accordance with these Terms and TriMet's linking policy. All other trademarks not owned by TriMet that appear on this Site are the property of their respective owners.

TRIMET

See where it takes you

Old logo - DO NOT USE

7. Disclaimer of warranties and limitation of liability

YOU AGREE THAT THE SERVICE IS PROVIDED TO YOU "AS IS" AND "AS AVAILABLE" WITHOUT ANY WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY AND NON-INFRINGEMENT. TriMet does not warrant that the Service will be available at any given time, secure, accurate or free of error. You use the Service at your own risk, and you assume the risk that the Service may provide incorrect information to you or your workers, as well as the risk that any material downloaded by you from the Service may cause loss of data or damage to your computer system.

YOU UNDERSTAND AND AGREE THAT IN NO EVENT WILL TRIMET BE LIABLE FOR ANY DIRECT OR INDIRECT DAMAGES, EVEN IF TRIMET IS AWARE OF THE POSSIBILITY OF SUCH

DAMAGES, INCLUDING WITHOUT LIMITATION LOSS OF PROFITS OR FOR ANY OTHER SPECIAL, CONSEQUENTIAL, EXEMPLARY OR INCIDENTAL DAMAGES, HOWEVER CAUSED, WHETHER BASED UPON CONTRACT, NEGLIGENCE, STRICT LIABILITY IN TORT, WARRANTY, OR ANY OTHER LEGAL THEORY, ARISING OUT OF OR RELATED TO YOUR USE OF THE SERVICE. THE PARTIES INTEND THAT THIS LIMITATION SHOULD APPLY EVEN IF IT CAUSES ANY WARRANTY TO FAIL OF ITS ESSENTIAL PURPOSE.

8. Indemnity

You agree to indemnify, defend and hold harmless TriMet and its officers, directors, and employees from and against all fines, suits, proceedings, claims, causes of action, demands, or liabilities of any kind or of any nature arising out of or in connection with your use of the Service.

9. Severability and waiver

The invalidity of any term or provision of these Terms will not affect the validity of any other provision. Waiver by TriMet of strict performances of any provision of these Terms will not be a waiver of or prejudice TriMet's right to require strict performance of the same provision in the future or of any other provision of these Terms.

10. Entire agreement

These Terms constitute the entire agreement between the parties as to their subject matter, and there are no other terms, conditions or obligations between the parties relating to the use of the Service, other than those contained in these Terms.

Privacy Statement

TRIMET MOBILE TICKETING SERVICE
PRIVACY POLICY
August 12, 2013

This privacy policy ("Policy") applies to the Tri-County Metropolitan Transportation District of Oregon ("TriMet") mobile ticketing service. It governs TriMet's collection, use, disclosure, protection, correction and deletion of personal information collected at the web site trimet.transitsherpa.com (the "Site"), and any mobile services or other applications operated by or for TriMet ("Service(s)"). The Policy is designed to tell you how we collect and use personal information (as defined below) so you can make an informed decision about using our Site and Service. Please read this Policy before using our Site or submitting any personal information to us.

TriMet complies with the requirements of the Children's Online Privacy Protection Act of 1998 (COPPA) and the FTC's Rule interpreting COPPA (16 CFR §512). The Site is not directed to children, and we do not knowingly collect any personal information on the Site from anyone under the age of 13 years. If we learn that a child under 13 years of age has provided us with personal information, we will delete this information from our databases. By using our Site, you represent that you are 14 years old or older and you consent to the information collection and use practices described herein. We reserve the right to change the provisions of this Policy at any time by posting a revised privacy policy on the Site and indicating on the privacy policy the date it was last updated. Your use of the Site following the posting of such changes or revised statement shall constitute your acceptance of any such changes. We encourage you to review our Policy whenever you

visit our Site to determine if any changes have been made and to make sure that you understand how any personal information you provide will be used.

WHAT IS "PERSONAL INFORMATION"?

As used herein, the term "personal information" generally means information that specifically identifies an individual (such as user's name, address, telephone number, e-mail address, geolocation, credit card or other account number) or that is associated with an identifiable person (such as device information, demographic information or information about a person's activities when such information is linked to personally identifying information). Personal information does not include "aggregate" information, which is data we collect about the use of the Site or categories of Site users, from which any personal information has been removed. Aggregate information may include statistical information concerning use of transportation services, or the pages on our Site that users visit most frequently. We collect aggregate data for a number of purposes, including to help us understand trends and user needs so that we can better consider new electronic newsletters, user alerts, products and services, and tailor existing electronic newsletters, user alerts, products and services to user desires. This Policy in no way limits or restricts our collection of aggregate information.

WHAT PERSONAL INFORMATION DO WE COLLECT?

We do not collect any personal information from mere visitors to the Site. Your email address may be collected when you send us an email as will your name and other personal information if you provide that with your email. When you subscribe to one of our electronic newsletters, you must provide your name and a valid email address. You may also provide your address, telephone number and organizational affiliation, and you may choose to create a password for managing your account.

We will also collect personal information in connection with registration of a mobile app and purchase of digital tickets for transit services. In this regard, you will be asked to provide contact information (such as name, address, email address, phone number, device type/model number and shipping address) and financial information (such as credit card number, expiration date and security code). This information is used for billing purposes and to fill orders. If we have trouble processing an order, the information may be used to contact you or to process a refund. If you decide to utilize the mobile ticketing service, you will be asked to register through the app or through the Site. Information that you provide may also be aggregated and used for

purposes of analysis and improvement of the Service once it is stripped of your personal information and it may then be shared with others.

If you use TriMet's mobile app, it may collect your GPS location or your device's unique identifier. It might also collect information regarding the type of mobile device you are using, or the version of the operating system your computer or device is running. This information may be maintained for purposes of tech support services. This information may also be aggregated and used for purposes of analysis and improvement of the Service once it is stripped of your personal information and it may then be shared with others.

If TriMet offers a managed account service, with autoload functionality, or loss protection features, and you choose to obtain such a managed account, you may be asked to provide contact information, and possibly financial information, depending on the level of service you select. TriMet will use the information you provide to register and service your managed account.

Any program offered by TriMet to provide users with useful transit alerts, such as information as to transit delays, would send such alerts in the form of email messages or text messages to the user's cellular phone or other mobile device. If you choose to participate in such a transit alert program, you will be asked to provide personal information, such as your email address or your cell phone number. We will only use this information to provide you with the alert services you have requested.

From time to time TriMet may conduct online and other surveys that customers may complete on a voluntary basis. Information collected through the surveys will only be used for the purpose of marketing or planning TriMet services unless you expressly agree otherwise.

To unsubscribe from TriMet email lists, simply click on the link labeled "Change your account settings" at the bottom of any email from us, or contact us at webadmin@trimet.org.

WHAT OTHER INFORMATION DO WE COLLECT?

When you visit our Site, some information is also automatically collected through the use of log files, such as your computer's or device's Internet Protocol (IP) address, your computer's or device's operating system, the browser type, the address of a referring web site and your activity on the Site. We use this information for purposes such as analyzing trends, administering the Site, improving customer service, diagnosing problems

with our servers, tracking user movement, and gathering broad demographic information for aggregate use. We may also automatically collect certain information through the use of "cookies." Cookies are small data files that are stored on a user's hard drive at the request of a Web site to enable the site to recognize users who have previously visited them and retain certain information such as customer preferences and history. If we combine cookies with or link them to any of the personally identifying information, we would treat this information as personal information. If you wish to block, erase, or be warned of cookies, please refer to your browser instructions or help screen to learn about these functions. However, if your browser is set not to accept cookies or if you reject a cookie, you will not be known to the Site when you return to it.

We may also use third parties to provide certain services, such as collecting, tracking and analyzing non-personally identifiable usage and statistical information from users, such as the user's browser type, operating system, browsing behavior and demographic information. These third parties may place cookies, web beacons or other devices on your computer or device to collect non-personal information which may be used, among other things, to deliver advertising targeted to your interests and to better understand the usage and visitation of our Site and the other sites tracked by these third parties. We will not allow such third parties to capture your personally identifying information unless you approve of such data gathering.

USAGE AND DISCLOSURE

The information covered by this Privacy Policy may be used in one or more of the following ways:

To send periodic emails

The email address you provide may be used to send you information and updates, if any, in addition to occasional TriMet news, updates, related product or service information, etc. You will be given an opportunity to opt out of such emails.

To respond to your requests, provide our services, process payments

We do not sell, rent, share, or disclose any personal information to others in ways different from what is disclosed in this Policy without first obtaining your consent, although we may provide aggregate information or other non-personal information to third parties without your authorization. We may share your contact information with third parties if you have indicated to us that you wish to receive information from such parties. In the event that we engage or partner with third party vendors, consultants or other service

providers in connection with the operation of our business ("Service Providers"), we may share personal information with such Service Providers who need access to such information to carry out their work for us. For example, we may use credit card processing or verification service companies to verify credit card information and process payments. We will require any such processing or verification services to comply with PCI privacy and security requirements. This Site and the Services are provided through the assistance of a third party vendor, GlobeSherpa, Inc. GlobeSherpa, Inc. utilizes your personal information solely for purposes of providing the mobile ticketing service and we do not approve its use of said information in any other way.

For compliance purposes

We also may disclose personal information (1) in connection with legal proceedings (such as false reimbursement claims made by TriMet patrons), or contemplated legal proceedings, that directly relate to such information; or in response to a subpoena or court order specifically requesting such information. And, we may disclose personal information to protect our customers' rights, property or safety, to protect our customers from fraudulent, abusive, or unlawful use of our Site, or in cases involving threat of imminent harm to you or others, in order to prevent or mitigate the threat. In any such case, we will seek to limit the scope of the disclosure and restrict such disclosures only to appropriate authorities, and will disclose only such personal information as is reasonably required to fulfill the purpose of the disclosure. In addition, unless instructed otherwise by a court or other authority with appropriate jurisdiction, we will undertake reasonable efforts to notify you of such disclosure or request for disclosure, and to provide you with this notice as far in advance of the disclosure as is reasonably practicable.

Please note: The Site may contain links to other sites. Please be aware that although we may participate in or utilize such other sites, we are not responsible for the privacy practices of such other sites. We encourage you to be aware when you leave our Site and to read the privacy policies of any Web site that collects personally identifiable information. Similarly, if you entered this Site through another Web site, we are also not responsible for the privacy practices of that site, and you should review the privacy policy of the originating site before providing any personal information to that site. This privacy policy applies solely to information collected by us.

Please also note: Persons who properly receive information in accordance

with the procedures set out in this Policy may be able to combine information they properly obtain from us with other information they independently possess concerning you. We will not be responsible for such later use of this information.

Public Records Law

Users should be aware that TriMet is a public agency and is subject to public records laws. Personal information provided by you may be subject to disclosure pursuant to public records laws unless the information meets certain statutory requirements. You should not provide personal information if you are concerned about disclosure of your information under those laws.

WHAT STEPS DO WE TAKE TO PROTECT YOUR INFORMATION ONLINE?

TriMet endeavors to secure your personal information from unauthorized access, use or disclosure by putting into place physical, electronic and managerial procedures to safeguard the information we collect through this Site and the Service. Please be aware, however, that despite our efforts, no security measures are perfect or impenetrable. Due to the nature of Internet communications and evolving technologies, we cannot provide, and disclaim, assurance that the information you provide to us will remain free from loss, misuse, or alteration by third parties, who, despite our efforts, obtain unauthorized access. If we detect an intrusion or other unauthorized access to or use of personal information, we will use commercially reasonable efforts to notify the individual(s) whose personal information has been compromised. You should also note that email is not secure, and you should not send any confidential or sensitive information to us via an unsecured email.

HOW CAN YOU CORRECT AND UPDATE YOUR PERSONAL INFORMATION OR OBTAIN ADDITIONAL INFORMATION

If you have any questions or comments about this Policy or the practices relating to this Site, or you wish to verify, correct or delete any personal information we have collected, please contact us at webadmin@trimet.org. To unsubscribe from TriMet newsletters, simply click on the link labeled "Change your account settings" at the bottom of any email from us, or contact us at webadmin@trimet.org.

CHOICE OF LAW AND JURISDICTION

This Site is operated for the benefit of TriMet from Portland, Oregon. This policy shall be construed in accordance with the laws of the State of Oregon,

without regard to any conflict of law provisions. Any dispute arising under this policy shall be resolved exclusively by the state or federal courts sitting in Multnomah County, Oregon.

Terms of Service

TRIMET MOBILE TICKETING TERMS OF SERVICE

August 12, 2013

These terms and conditions ("Service Terms") govern your ("you" or "your") access to, and use of, the web site at trimet.transitsherpa.com and the mobile ticketing services ("Services") provided by the Tri-County Metropolitan Transportation District of Oregon ("TriMet"), including, without limitation, any software applications loaded onto mobile devices. These Service Terms do not alter in any way the terms of any written agreement signed by you and TriMet. If you are using the Services on behalf of any entity, you represent and warrant that you are authorized to accept these Service Terms on such entity's behalf and the term "you" shall refer to you personally and such entity.

TriMet reserves the right to change or modify these Service Terms at any time and in its sole discretion, upon ten (10) days notice by email. If you do not accept such modified terms, you must provide TriMet email notice of termination within such ten (10) day period or be bound by such modified terms.

If you have any questions regarding the use of the Services, please refer first to the support section of the Site. All other questions or comments about the Services or its contents should be directed to webadmin@trimet.org.

You agree to comply with, and to ensure compliance with, all laws, ordinances and regulations applicable to your activities in using the Services.

You certify that you are at least 14 years of age.

1. Registration.

If you wish to utilize the Services, you will be required to register by providing information about yourself and, if you are registering on behalf of an entity, information about that entity (such as identification, and contact details). You agree that any such information you provide is accurate, complete and updated. Failure to do so constitutes a breach to these Service Terms and may result in a termination of your account and access to the Services. You are responsible for maintaining the security and confidentiality of your account password. You are also solely responsible for all activities that occur

through your User ID and password. You agree not to access or use, or attempt to access or use, the Services or any part thereof using the identity or the Registration Data of any person other than yourself. You agree to immediately notify TriMet of any unauthorized use of your User ID or password. From time to time, you may be asked to confirm your account via an email message. If such account is not reconfirmed, the account may be deleted by TriMet. Once your account has been deleted, your information may remain on the Services, or be removed by TriMet. Please read our Privacy Policy, which describes the personally identifiable information we collect, use, disclose, manage and store.

2. Methods of Payment.

TriMet accepts the following methods of payment for ticket purchases: MasterCard, Visa, American Express, Discover and debit via online banking. All ticket prices are stated in U.S. Dollars.

3. Pricing, Availability; Purchase Confirmation; Refunds.

If you do not receive (i) a message containing your ticket, and (ii) a confirmation number for your ticket order (in the form of a confirmation page or purchase receipt) after submitting payment information, or if you experience an error message or service interruption after submitting payment information, it is your responsibility as the customer to confirm with TriMet's customer service department whether or not your order has been placed. Only you may be aware of any problems that may occur during the purchase process. TriMet will not be responsible for losses (monetary or otherwise) if you fail to receive the tickets and/or an order confirmation and such failure is not caused by the Services.

4. Violations of TriMet Code/Law; No Redemption Value.

Use of the TriMet District Transit System is subject to the TriMet Code and applicable law. TriMet reserves the right, without refund of any amount paid, to prosecute and to impose any penalties allowed by the TriMet Code or law, including but not limited to exclusion and citation, upon any person whose conduct violates the TriMet Code or applicable law while on the District Transit System. You agree to fully cooperate with TriMet Inspectors and peace officers upon demand to exhibit proof of fare payment for your mobile ticket in accordance with TriMet Code Chapter 29 Proof of Fare Payment. You are solely responsible at all times for the proper functioning of your mobile phone. It is your responsibility to ensure that the mobile phone is sufficiently charged to clearly and legibly display the mobile ticket and to otherwise exhibit proof of fare payment in accordance with TriMet Code

Chapter 29 Proof of Fare Payment, as many times as required for the duration of your use of the District Transit System. You understand that you will be subject to penalties, including but not limited to citation and exclusion, for failure to exhibit proof of fare payment.

A ticket is not redeemable for cash.

5. Code of Conduct.

In connection with your use of the Services, you agree that you will not:

- Restrict or inhibit any other visitor or user from using the Services, including, without limitation, by means of "hacking" or defacing any portion of the Services;
- Use the Services or the Materials (as defined below) for any unlawful purpose;
- Transmit any software or other materials that contain any viruses, worms, Trojan horses, defects, date bombs, time bombs or other items of a destructive nature;
- Modify, adapt, sub-license, translate, sell, reverse engineer, decompile or disassemble any portion of the Services or otherwise attempt to derive any source code or underlying ideas or algorithms of any part of the Services;
- Remove any copyright, trademark or other proprietary rights notices contained on the Services;
- "Frame" or "mirror" any part of the Services;
- Use any robot, spider, offline reader, site search/retrieval application or other manual or automatic device or process to retrieve, index, data mine or in any way reproduce or circumvent the navigational structure or presentation of the Services or its contents without our prior written consent; or
- Take any action that imposes or may impose (in TriMet's sole discretion) an unreasonable or disproportionately large load on our (or our third party providers') infrastructure.

6. Ownership and Restrictions on Use.

The information and materials provided on or through the Services, including any data, text, designs, graphics, images, photographs, illustrations, audio and video clips, logos, icons and links (collectively, the "Materials") are owned exclusively by TriMet or its licensors, and are intended to educate and inform you about the products and services offered or described on the Services. Subject to your compliance with these Service Terms, you may

download one (1) copy of any Materials displayed on the Services, and you may use such downloaded Materials solely for your personal, non-commercial use (you may not resell the Services), provided that you retain all copyright and other proprietary notices contained therein. TriMet cannot guarantee that technical difficulties will not occur during the download of the Materials or that the Materials will download successfully. Subject to your compliance with these Service Terms, we grant you a limited license to use the Services and Materials; provided that you may not use, reproduce, modify, display, publicly perform, distribute, create derivative works of or circumvent any technological measure that effectively controls access to the Services and/or Materials in any way including, without limitation, by manual or automatic device or process, for any purpose. Use of the Services and Materials for any purpose other than as expressly authorized in these Service Terms is a violation of our copyrights and other proprietary rights, and is strictly prohibited.

The Services, including all software, databases, proprietary information and Materials (and any intellectual property and other rights relating thereto) including, without limitation, the selection, sequence and "look and feel" and arrangement of items, is owned and operated by TriMet and its licensors and will remain the property of TriMet and its licensors. The Services are protected by U.S. and international copyright, trademark and other laws, and you acknowledge that these rights are valid and enforceable. You further acknowledge that you do not acquire any ownership rights by using the Services or the Materials.

The trademarks, logos, and service marks displayed on the Services (collectively the "Trademarks") are the registered and unregistered trademarks of TriMet and GlobeSherpa, Inc. and their licensors and suppliers, and others. The Trademarks, whether registered or unregistered, may not be used in connection with any product or service that is not offered by TriMet, in any manner that is likely to cause confusion with customers, or in any manner that disparages TriMet. Nothing contained on the Services should be construed as granting, by implication, estoppel or otherwise, any license or right to use any Trademark without the express written permission of TriMet, TriMet's licensors or suppliers, or the third party owner of any such Trademark. Misuse of any Trademarks is prohibited, and TriMet will aggressively enforce its intellectual property rights in such Trademarks, including via civil and criminal proceedings.

7. Making Purchases.

If you wish to purchase products or services described (each such purchase, a "Transaction"), you will be asked to supply certain information applicable to your Transaction, including, without limitation, credit card and other information. You understand that any such information will be treated by TriMet in the manner described in our Privacy Policy. You agree that all information that you provide in connection with your purchase will be accurate, current and complete. You agree to pay all charges incurred by you or any users of your account and credit card (or other applicable payment mechanism) at the price(s) in effect when such charges are incurred. You will also be responsible for paying any applicable taxes relating to your purchases. The sale or purchase of tickets may be regulated by certain state, county and city laws or regulations. You acknowledge that complying with laws is your responsibility. WE WILL COMPLY WITH LAW ENFORCEMENT OFFICIALS AND MAY PROVIDE THEM WITH ALL INFORMATION YOU SUBMIT TO US TO ASSIST IN ANY INVESTIGATION OR PROSECUTION THEY MAY CONDUCT. You represent and warrant that all information you provide, including but not limited to all information concerning your name, address, credit card number, and other identifying information of any nature will be true, complete and correct, and that you will update all information as it changes. You grant TriMet the right to provide any information you submit to third parties for purposes of facilitating the completion of Transactions initiated by you or on your behalf. Verification of information may be required prior to the acknowledgment or completion of any Transaction.

8. Information Provided by TriMet.

Although TriMet strives to provide Materials that are both useful and accurate, the nature of the data and other information contained on the Services is subject to frequent change. In addition, the facts and circumstances of every situation differ. Accordingly, although TriMet endeavors to use reasonable care in assembling the Materials, the Materials may not be up-to-date, accurate or complete.

9. Consent to Receive Emails and Notice.

As long as you maintain an account, you may not "opt out" of receiving account-related emails from TriMet. The parties hereto may give legal notice by means of electronic mail, which electronic mail shall be considered delivered when sent. The notice address of TriMet shall be webadmin@trimet.org (or such other address as is provided by TriMet to you) via email at your Notice address and your address for the receipt of

notices pursuant to this Agreement shall be the current email address listed by you in your account profile. You also agree, unless you opt out, to receive marketing emails related to the Services.

10. Linking and Hyperlinking.

You are granted a limited, non-exclusive right to create a text hyperlink to the Services, provided such link does not portray TriMet, any of its products and services, in a false, misleading, or otherwise defamatory manner and provided further that the linking site does not contain any illegal material. This limited right may be revoked at any time. You may not use a TriMet logo or other proprietary graphic to link to the Services without the express written permission of TriMet. Further, you may not use, frame or utilize framing techniques to enclose any TriMet trademark, logo or other proprietary information, including the images found on the Services, the content of any text or the layout/design of any page or form contained on a page on the Services without TriMet express written consent. Except as noted above, you are not conveyed any right or license by implication, estoppel or otherwise in or under any patent, trademark, copyright or proprietary right of TriMet or any third party.

11. Links and Third Party Content.

TriMet may provide links to Web pages and content of third parties as a service to those interested in such links and content, and TriMet may post third party content or allow users to post their content. TriMet does not have resources to constantly monitor or have ultimate control over any Third Party Content or third party websites. TriMet does not endorse or adopt any Third Party Content or third party websites and can make no guarantee as to its accuracy or completeness. TriMet does not represent or warrant the accuracy of any information contained therein and undertakes no responsibility to update or review any Third Party Content or third party Websites. Users use these links, Third Party Content and third party Websites at their own risk. When you leave the Services, you should be aware that our terms and policies no longer govern. You should review the applicable terms and policies, including privacy and data gathering practices, of any service to which you navigate from the Services.

12. Third Party Goods and/or Services.

The Services may also provide information regarding or link to certain applications and goods and/or services provided or offered by third parties (collectively the "Third-Party Goods and Services"). TriMet is merely an information provider and is not a referral service, and it does not recommend

or endorse any such Third-Party Services or monitor or have any control over such Third Party Goods and/or Services. Therefore, TriMet makes no guarantee, representation or warranty of any kinds as to the quality, competency, value, reliability, responsiveness, accuracy or completeness of any such Third-Party Services or the results obtained therefrom, and TriMet assumes no responsibility or liability for any Third Party Goods and/or Services or for the actions or failure to act of those providing such Third-Party Services. You assume full responsibility for your use of any such Third-Party Services, and TriMet is not responsible or liable for any Third-Party Services. In the event of a dispute between any consumer and vendor, the parties will work out the dispute themselves.

13. Advertisements and Promotions.

TriMet may run advertisements and promotions from third parties on the Services. Your business dealings or correspondence with, or participation in promotions of, advertisers other than TriMet, and any terms, conditions, warranties or representations associated with such dealings, are solely between you and such third party. TriMet is not responsible or liable for any loss or damage of any sort incurred as the result of any such dealings or as the result of the presence of such third party advertisers on the Services.

14. Termination.

These Service Terms shall remain effective until terminated in accordance with its terms. We reserve the right to immediately terminate these Service Terms, and/or your access to and use of the Services or any portion thereof, at any time and for any reason, with or without cause. Upon termination of these Service Terms, your right to use the Services shall immediately cease, and you shall destroy all Materials obtained from the Services and all copies thereof, whether made under these Service Terms or otherwise. You agree that any termination of your access to or use of the Services may be effected without prior notice, and that TriMet may immediately deactivate or delete your password and user name, and all related information and files associated with it, and/or bar any further access to such information or files. You agree that TriMet shall not be liable to you or any third party for any termination of your access to the Services or to any such information or files, and shall not be required to make such information or files available to you after any such termination.

Violations of these Service Terms, including unauthorized use of the Services, may be investigated and appropriate legal action may be taken, including without limitation civil, criminal and injunctive redress. You agree

that monetary damages may not provide a sufficient remedy to TriMet for violations of these Service Terms and you consent to injunctive or other equitable relief for such violations.

TriMet is not required to provide any refund to you if it exercises any of its rights or remedies because you have violated these Service Terms or any of TriMet's rights. Additionally, we reserve the right, in our sole discretion, to modify, suspend or discontinue any part of this the Services at any time, with or without notice to you. We also reserve the right, in our sole discretion, to impose limits on certain features and services and to restrict access to any part or to all of the Services without notice to you. We shall not be liable to you or any third party for any claim or cause of action arising out of our exercise of the foregoing rights.

15. WARRANTY DISCLAIMER.

THE SERVICES, THE MATERIALS ON THE SERVICES, AND ANY PRODUCT OR SERVICE OBTAINED THROUGH THE SERVICES IS PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, TRIMET AND ITS LICENSORS AND CLIENTS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE SERVICES, THE MATERIALS, AND ANY PRODUCT OR SERVICE OBTAINED THROUGH THE SERVICES, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF TITLE, NON-INFRINGEMENT, ACCURACY, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTIES THAT MAY ARISE FROM COURSE OF DEALING, COURSE OF PERFORMANCE OR USAGE OF TRADE. Applicable law may not allow the exclusion of implied warranties, so the above exclusions may not apply to you. NEITHER TRIMET NOR ITS LICENSORS OR CLIENTS WARRANT THAT YOUR USE OF THE SERVICES WILL BE UNINTERRUPTED, ERROR-FREE OR SECURE, THAT DEFECTS WILL BE CORRECTED, OR THAT THE SERVICES, THE SERVER(S) ON WHICH THE SERVICES ARE HOSTED IS FREE OF VIRUSES OR OTHER HARMFUL COMPONENTS. YOU ACKNOWLEDGE THAT YOU ARE RESPONSIBLE FOR OBTAINING AND MAINTAINING ALL TELEPHONE, COMPUTER HARDWARE AND OTHER EQUIPMENT NEEDED TO ACCESS AND USE THE SERVICES, AND ALL CHARGES RELATED THERETO. YOU ASSUME ALL RESPONSIBILITY AND RISK FOR YOUR USE OF THE SERVICES AND YOUR RELIANCE THEREON. NO OPINION, ADVICE OR STATEMENT OF TRIMET, WHETHER MADE ON

THE SERVICES OR OTHERWISE, SHALL CREATE ANY WARRANTY. TRIMET DOES NOT WARRANT, ENDORSE, GUARANTEE, OR ASSUME RESPONSIBILITY FOR ANY PRODUCT OR SERVICE ADVERTISED OR OFFERED BY A THIRD PARTY THROUGH THE SERVICES OR ANY HYPERLINKED SITE, OR FEATURED IN ANY BANNER OR OTHER ADVERTISING, AND TRIMET WILL NOT BE A PARTY TO OR IN ANY WAY MONITOR ANY TRANSACTION BETWEEN YOU AND THIRD-PARTY PROVIDERS OF PRODUCTS OR SERVICES. AS WITH THE PURCHASE OF A PRODUCT OR SERVICE THROUGH ANY MEDIUM OR IN ANY ENVIRONMENT, YOU SHOULD USE YOUR BEST JUDGMENT AND EXERCISE CAUTION WHERE APPROPRIATE. **YOUR USE OF THE SERVICES AND ANY MATERIALS PROVIDED THROUGH THE SERVICES ARE ENTIRELY AT YOUR OWN RISK.** YOU ACKNOWLEDGE AND AGREE THAT NEITHER TRIMET NOR ITS LICENSORS OR CLIENTS IS RESPONSIBLE FOR ANY CONTACT OR INTERACTION BETWEEN YOU AND ANY OTHER USER OF THE SERVICES AND THAT YOU BEAR THE SOLE RISK OF TRANSMITTING THROUGH THE SERVICES ANY CONTENT, INCLUDING INFORMATION WHICH IDENTIFIES YOU OR YOUR LOCATION.

16. Limitation of Liability.

NEITHER TRIMET NOR ANY OF OUR AFFILIATES, LICENSORS, CLIENTS, SUPPLIERS, ADVERTISERS OR SPONSORS, NOR OUR OR THEIR DIRECTORS, OFFICERS, EMPLOYEES, CONSULTANTS, AGENTS OR OTHER REPRESENTATIVES ("TRIMET RELEASEES"), ARE OR WILL BE RESPONSIBLE OR LIABLE TO YOU OR TO ANY THIRD PARTY FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, EXEMPLARY, PUNITIVE OR OTHER DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, LOSS OF DATA OR LOST PROFITS), UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER THEORY ARISING OUT OF OR RELATING IN ANY WAY TO THE SERVICES AND/OR MATERIALS CONTAINED ON THE SERVICES, ANY LINKED SITE OR ANY PRODUCT OR SERVICE PURCHASED THROUGH THE SERVICES. WITHOUT LIMITING THE FOREGOING, YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT THE TRIMET RELEASEES SHALL HAVE NO LIABILITY OR RESPONSIBILITY WHATSOEVER FOR (I) PERSONAL INJURY OR PROPERTY DAMAGE, OF ANY NATURE WHATSOEVER, WHETHER ARISING IN CONTRACT OR IN TORT, RESULTING FROM YOUR ACCESS TO AND USE OF OUR SITE, INCLUDING ANY CLAIM, CAUSE OF ACTION, OBLIGATION, LIABILITY,

RIGHT, OR REMEDY WHETHER OR NOT ARISING FROM THE NEGLIGENCE OF TRIMET OR ITS RELEASEES, (II) ANY UNAUTHORIZED ACCESS TO OR USE OF OUR SECURE SERVERS AND/OR ANY AND ALL PERSONAL INFORMATION AND/OR FINANCIAL INFORMATION STORED THEREIN, (III) ANY INTERRUPTION OR CESSATION OF TRANSMISSION TO OR FROM OUR SITE, (IV) ANY BUGS, VIRUSES, WORMS, TROJAN HORSES, DEFECTS, DATE BOMBS, TIME BOMBS OR OTHER ITEMS OF A DESTRUCTIVE NATURE WHICH MAY BE TRANSMITTED TO OR THROUGH OUR SITE BY ANY THIRD PARTY, (V) ANY ERRORS, MISTAKES, INACCURACIES OR OMISSIONS IN ANY MATERIALS, OR FOR ANY LOSS OR DAMAGE OF ANY KIND INCURRED AS A RESULT OF THE USE OF ANY MATERIALS POSTED, EMAILED, TRANSMITTED OR OTHERWISE MADE AVAILABLE VIA THE SERVICES, AND/OR (VI) THE FAILURE OF A TRANSIT SYSTEM TO HONOR A TICKET. YOUR SOLE AND EXCLUSIVE REMEDY FOR DISSATISFACTION WITH THE SERVICES OR MATERIALS OR ANY LINKED SITE IS TO STOP USING THE SERVICES, MATERIALS, OR LINKED SITE, AS APPLICABLE. THE MAXIMUM LIABILITY OF TRIMET AND ITS LICENSORS, AND YOUR SOLE AND EXCLUSIVE REMEDY, FOR ALL DAMAGES, LOSSES SUFFERED BY YOU AND CAUSES OF ACTION, WHETHER IN CONTRACT, TORT (INCLUDING, WITHOUT LIMITATION, NEGLIGENCE) OR OTHERWISE, SHALL BE ONE HUNDRED DOLLARS ($100.00).

17. Indemnification.

You agree to indemnify, defend and hold TriMet, its affiliates, licensors, clients, suppliers, advertisers and sponsors, contractors and their respective directors, officers, employees, consultants, agents and other representatives, harmless from and against any and all claims, damages, losses, costs (including reasonable attorneys' fees) and other expenses that arise directly or indirectly out of or from (a) your breach of these Service Terms; (b) any allegation that any materials you submit to us or transmit to the Services infringe or otherwise violate the copyright, trademark, trade secret or other intellectual property or other rights of any third party; and/or (c) your activities in connection with the Services.

18. Privacy.

We believe that your privacy and the privacy of all our users is important. These Service Terms are subject to the Privacy Policy, which is hereby incorporated by reference.

19. Interstate Nature of Communications.

You acknowledge that in using TriMet Services you will be causing communications to be sent through interstate telecommunications networks, which are governed by federal law pursuant to the interstate commerce clause of the US Constitution. Even communications that seem to be intrastate in nature can result in the transmission of interstate communications regardless of where you are physically located at the time of transmission. You acknowledge that use of the Services results in interstate data transmissions.

20. Assignment; Change in Control.

This Agreement may not be assigned by you without the prior written approval of TriMet but may be assigned without your consent by TriMet to (i) a parent or subsidiary, (ii) an acquirer of assets, or (iii) a successor by merger. Any attempt at improper assignment shall be void.

21. Severability.

If any of these Service Terms or the Terms of Service should be determined to be invalid, illegal or unenforceable for any reason by any court of competent jurisdiction then such term shall be enforced only to the extent it is enforceable and the remaining terms shall survive and remain in full force and effect and continue to be binding and enforceable.

22. Waiver.

No waiver of any term, provision or condition of this Agreement, whether by conduct or otherwise, in any one or more instances, shall be deemed to be, or shall constitute, a waiver of any other term, provision or condition hereof, whether or not similar, nor shall such waiver constitute a continuing waiver of any such term, provision or condition hereof. No waiver shall be binding unless executed in writing by the party making the waiver.

23. Force Majeure.

If the performance of the Services or any part of this Agreement by either party is prevented, hindered, delayed or otherwise made impracticable by reason of any flood, riot, fire, judicial or governmental action, labor disputes, act of God or any other causes beyond the control of either party, that party shall be excused from such to the extent that it is prevented, hindered or delayed by such causes.

24. Miscellaneous.

These Service Terms constitute the entire agreement between you and TriMet and supersede any prior written or oral agreement with regard to the Services. Any and all claims, causes of action or disputes (regardless of

theory) between you and TriMet arising out of or related to the Service Terms, the Services or content accessed through the Services shall be governed by the laws of the State of Oregon without regard to conflict or choice of law principles. You and TriMet agree that any such claims, causes of action or disputes shall be brought exclusively in courts located within Multnomah County, Oregon, and you and TriMet agree to submit to the personal and exclusive jurisdiction of such courts. You further agree that, regardless of any statute or law to the contrary, you must file any such claim or cause of action within one year after such claim or cause of action arose or be forever barred.

25. Questions.

If you have any questions; comments or complaints regarding these Service Terms or the Services, feel free to contact us at: webadmin@trimet.org.

Federal Reserve Payments Study, Transit System Operator, Electronic Fares Collected Survey, Calendar Year 2015 12

FR 3066b
OMB No. 7100-0351
Approval expires March 31, 2019

The Federal Reserve Payments Study

Transit System Operator
Electronic Fares Collected Survey

Survey Period:
Calendar Year 2015

Surveys of the number and dollar value of different types of electronic payment transactions in the United States

Please complete this survey by June 30, 2016

Contact information is for survey administration purposes only:

Organization Name	**VIA Metropolitan Transit**
Contact Name	**Barney Sifuentes**
Telephone Number	**210-362-2178**
Participant email	**barney.sifuentes@viainfo.net**

Instructions

The Federal Reserve *2016 Networks, Processors, and Issuers Payments Surveys (NPIPS)* collects the number and dollar value of different types of ***domestic and cross-border*** electronic payment transactions and related information including fraud from ***U.S.-domiciled accounts*** during ***calendar year 2015***, and made by ACH, credit card, debit card, prepaid card, or alternative payment initiation methods. Data from your response will contribute to estimates of the national aggregate number and value of electronic payments made by these transaction methods. The Federal Reserve will compare the results from this 2016 study to those of previous triennial studies conducted from 2001 to 2013.

Confidentiality

Any information you provide for this survey is strictly confidential. Individual responses to the survey will not be shared with the public or the industry.

Your participation

To achieve the most reliable results, it is important that you respond completely and accurately. **Please leave no survey item blank.**

If you would prefer an electronic version of the survey, visit http://www.frbnpips.net/forms.html to download either a MS-Word or MS-Excel versions of the survey or send an email to ebachelder@frbnpips.net to request one.

General instructions for numeric fields

There are **three possible ways** to respond to a survey item that requests a numeric value:

If your institution has volume for the item requested and the volume is known or can be accurately estimated, **enter the amount**. (**Enter "0" if the amount equals zero.**)

If your institution has volume for the item requested but the volume is unknown and cannot be accurately estimated, **enter "NR"** (not reported). (**Do not enter "0" if the volume exists but the amount is unknown.**)

If your institution does not have volume for the item requested (i.e., the item requested does not apply to your institution), **enter "0"**.

Definitions and examples

For this study, we are seeking to count the number and dollar value of customer payments **collected** (fares and fees) by Transit System Operators in the United States during the calendar year 2015. The survey asks about fare media used to collect payment from riders. It does **not** ask about payments made by transit operators.

Definitions and examples can be found in the glossary. Several terms are defined on page 5. Please visit http://www.frbnpips.net/forms.html to download a copy of the glossary that you can use to complete the survey.

Submitting your completed survey

You may submit your completed paper response by mail or fax or email a PDF, word or excel version of your survey response.

By Fax 1-866-434-5583 (must dial the "1")

By Mail: Blueflame Consulting
80 Warwick Road
Melrose, MA 02176

email: survey@frbnpips.net

If for any reason you cannot provide complete data, or if you have any questions or concerns, please contact: **ebachelder@frbnpips.net** or call Blueflame Consulting at (781) 662-8584.

Transit System Operator Electronic Fares Collected Survey

Calendar year 2015 transit operator transactions (trips)	Number	Value ($)
1. Total transactions (trips) *Please provide unlinked rides, including complete fixed route and paratransit.*	41,546,790	22,729,368
1a. Cash payment	23,703,473	13,469,786
1b. General-purpose card (credit, debit or prepaid) payment	0	0
1c. Payment made by fare media issued by your organization	0	0
1c.1. Chip (e.g., contactless card/token) or smart media	0	0
1c.1.1. Unlimited rides for a specified time period	0	0
1c.1.2. Other_____ *Please specify. This may include 1 time pass, 7-day pass, etc.*		
1c.2. No chip (e.g., magnetic stripe pass, metal token)	17,843,317	9,259,582
1c.2.1. Unlimited rides for a specified time period	15,684,210	7,165,185
1c.2.2. Other 1 time ticket & contract *Please specify. This may include 1 time pass, 7-day pass, etc.*	2,159,107	2,094,397
1d. Payment made by mobile device	0	0
1e. Payment made by other fare media	0	0

Funding method	Number	Value ($)
2. Total funding for fare media issued by your organization *Please refer to question 1c above ONLY.*	17,843,317	9,259,582
2a. Cash	3,211.797	1,666,725
2b. Check	10,705,990	5,555,749
2c. General-purpose card (credit, debit, or prepaid)	3,925,530	2,037,108
2d. ACH	0	0
2e. Other_____ *Please specify*	0	0

Transit System Operator Electronic Fares Collected Survey

Preferred basis for reporting card activity

3. **Active fare media** are fare media that were used to make at least one purchase or bill payment over a period of time. On which basis would you prefer to report active fare media below? If you have no preference, please choose 1 year.

[ ] 1 month [ ] 3 months
[ ] 6 months [x] 1 year
[ ] Other, please describe

Number of fare media issued by your organization outstanding

	Active fare media	Total fare media
4. **Number of fare media issued by your organization for both active and total fare media outstanding as of December 31, 2014**	2,724,281	3,243,655
4a. **Chip (e.g., contactless card/token) or smart media**	0	0
4a.1. **Unlimited rides for a specified time period**	0	0
4a.2. **Other**_____ *Please specify. This may include 1 time pass, 7-day pass, etc.*	0	0
4b. **No chip (e.g., magnetic stripe pass, metal token)**	2,724,281	3,243,655
4b.1. **Unlimited rides for a specified time period**	235,185	288,135
4b.2. **Other** Single ride tickets *Please specif. This may include 1 time pass, 7-day pass, etc.*	2,489,656	2,955,520
5. **Number of fare media issued by your organization for both active and total fare media outstanding as of December 31, 2015**	2,365,763	2,792,029
5a. **Chip (e.g., contactless card/token) or smart media**	0	0
5a.1. **Unlimited rides for a specified time period**	0	0
5a.2. **Other**_____ *Please specify. This may include 1 time pass, 7-day pass, etc.*	0	0
5b. **No chip (e.g., magnetic stripe pass, metal token)**	2,365,763	2,792,029
5b.1. **Unlimited rides for a specified time period**	209,855	257,259
5b.2. **Other** Single ride tickets *Please specify. This may include 1 time pass, 7-day pass, etc.*	2,155,908	2,534,770

Transit System Operator Electronic Fares Collected Survey

Fraudulent transactions	Number	Value ($)
6. Total fraudulent transactions (trips)	NR	NR
6a. Cash payment	NR	NR
6b. General-purpose card (credit, debit or prepaid) payment	NR	NR
6c. Payment made by fare media issued by your organization	NR	NR
6c.1. Chip (e.g., contactless card/token) or smart media	0	0
6c.1.1. Unlimited rides for a specified time period	0	0
6c.1.2. Other_____ *Please specify. This may include 1 time pass, 7-day pass, etc.*	0	0
6c.2. No chip (e.g., magnetic stripe pass, metal token)	NR	NR
6c.2.1. Unlimited rides for a specified time period	NR	NR
6c.2.2. Other Single ride tickets *Please specify. This may include 1 time pass, 7-day pass, etc.*	NR	NR
6d. Payment made by mobile device	0	0
6e. Payment made by other fare media	0	0

Definitions of Key Terms

Fixed route service is transit service provided on a repetitive, fixed schedule basis along a specific route with vehicles stopping to pick up or deliver passengers at designated locations.

Question	
1	**Total Transactions (trips)** ***Unlinked*** **passenger trips** count each boarding as a separate trip regardless of transfers
1c	**Fare media** includes any means of payment or proof of payment including tickets, tokens, transfers, passes, fare cards, and smart cards.
1c.1	**Chip or Smart media** is chip-based devices in a variety of form factors, including plastic cards, key fobs, and mobile phones.
1d	**Mobile payments (m-payments)** are payment transactions executed on a mobile device, whether remote such as "in-app purchase", or at a point-of-sale (POS).
6	**Fraudulent transaction** is an unauthorized transaction committed by a third-party who is not the authorized accountholder or cardholder that result in losses incurred.