



DATE: 4/29/25

TO: Robert Gleason, Director, Purchasing Division

THRU: John Pokryfke

FROM: James Walker

PROJECT TITLE: Transaction Network Services (TNS)

REQUISITION NO. AVA0003210

SOURCE/BRAND NAME: Transaction Network Services

SOLE SOURCE/SOLE BRAND/ONLY ONE REASONABLE SOURCE REQUEST



SOLE SOURCE



SOLE BRAND



ONLY ONE REASONABLE
SOURCE

I. REQUEST: Provide a description of the features of the product/service or Scope of Work.

TNS is a software company that processes credit card payments, pre-authorisations and captures, performs refund/reversal, provides summary and detailed reports and accept transactions through a merchant facility. Additionally, it is a cloud hosted application for the processing of all credit card transactions.

II. JUSTIFICATION: Please check all boxes that describe your reason(s) for determining that only one source or brand is reasonably available.

Sole Source/Uniqueness



Proprietary Item - this vendor/source has the only rights to provide this service or commodity. A letter from the manufacturer or authorizing entity is included in this request.



Technology Improvements - updates or upgrades to an existing system, software, software as a service (SaaS), hardware purchases.



Engineering Direction - engineering drawing or specification identifies product; "no substitutes or equivalents will be acceptable."



Only qualified supplier - reliability and maintainability of the product or service would be degraded unless specified supplier is used; may void warranty. This request includes a copy of the current warranty information.

☐ Other/or Additional information - the County requires this sole source purchase for the following reasons.

The new equipment installed by Designa Access Corporation only integrates with Transaction Network Services (TNS). It's a cloud hosted application for the processing of credit card transactions of the ADVAM payment processing system. The aim is to simplify complex payment infrastructure to allow secure transaction processing.

Business Case (Only One Reasonable Source¹ or Only One Reasonable Brand)

- ☒ Operational Compatibility - replacement parts from alternate suppliers are not interchangeable with original part and causes equipment incompatibility. Previous findings and/or documentation is included with this request.
- ☒ Ease of Maintenance - maintenance or retooling prohibits competition. Section III, Comparative Market Research includes estimated costs associated with changing current source and/or brand.
- ☒ Follow-On - potential for continued development or enhancement with same supplier and eliminates costs incurred by using different supplier. Section III, Comparative Market Research includes estimated costs for replacing current or existing system.
- ☐ Complies with existing community and safety standards, and/or laws, rules, and regulations.
- ☒ Other/or additional information - using this only one reasonable source, only one reasonable brand purchase benefits the County for the following reasons:

The Designa processing equipment integrates solely with the reasonably brand TNS system and ADVAM payment processing. If the Designa equipment is not connected to the TNS processor, additional equipment will be required causing an increase in cost of retrofitting of all payment processing equipment campus wide and additional maintenance.

III. COMPARATIVE MARKET RESEARCH: Provide a detailed source or market analysis for justification of sole source/brand or most reasonable source (attach extra sheets as needed).

Estimated project value: \$170,000 Contract length (if applicable): 10 years

Has this commodity or service been previously provided to the County? ☒ Yes ☐ No

If yes, provide the following and attach any supporting documentation (e.g., previous approved memoranda):

Vendor name and date Datacap Method of Procurement via HUB Parking agreement

What is the current contract (Procurement Catalog) or purchase order number? N/A

Expenditures to date: N/A

Will this procurement utilize any local/state/federal grant funding? ☐ Yes ☒ No

If yes, attach any supporting documentation (e.g., grant agreement).

If this is a sole brand, is there an "authorized" dealers/resellers list? ☐ Yes ☒ No

If yes, provide the manufacturer's "authorized" dealers/resellers list.

¹ Commonly known as Most Reasonable Source

Cost/Benefit Analysis: What would the cost be to utilize an alternate vendor or source? This explanation should include the savings and/or additional costs to the County by not using the preferred vendor or source. Attach additional sheets if needed.

CERTIFICATION: I have thoroughly researched the sole source, sole brand, only one reasonable source, or only one reasonable brand justification and fully understand the implications of Section 838.22 of the Florida Statutes:

(2) "It is unlawful for a public servant or a public contractor who has contracted with a governmental entity to assist in a competitive procurement to knowingly and intentionally obtain a benefit for any person or to cause unlawful harm to another by circumventing a competitive solicitation process required by law or rule through the use of a sole-source contract for commodities or services".

(5) "Any person who violates this section commits a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084".

I. Dedrie Registe

D. Dedrie Registe

5/30/25

REQUESTOR/EVALUATOR (PRINT)

REQUESTOR/EVALUATOR (SIGN)

DATE

John POKRYKE

John POKRYKE

7/23/25

DEPT/DIV DIRECTOR OR
DESIGNEE (PRINT)

DEPT/DIV DIRECTOR OR DESIGNEE
(SIGN)

DATE

PURCHASING DIVISION USE ONLY

The Purchasing Agent has reviewed the request and has completed the required due diligence per the Procurement Code Section(s) 21.25 and 21.26. The Purchasing Agent recommends the following:

- | | | | |
|---|--|--|---------------------------------|
| ☒ Sole Source | ☐ Sole Brand | ☐ Only One Reasonable Source/Brand ² | ☐ Reject |
| ☐ Authorization to Negotiate | ☐ Standardization | ☐ Board Award | |

Attachments

- | | |
|--|--|
| ☐ Request for Information | ☐ Previous Approved Documentation |
| ☐ Vendor Letter | |

² As per Florida Statute 287.057(3)(c), FLL projects valued $\geq$ \$325,000 require 15 business day posting of intended sole source designation

Additional Information (e.g., Number, opening date, # of responses, Agency reviewed yes/no):

The Purchasing Agent affirms that the required due diligence has been completed through Request for Information (RFI) No. PNC544999F1 (Exhibit 1) and recommends approval of this request. RFI No. PNC544999F1 was advertised on May 2, 2025 and opened on May 23, 2025 with no responses received. Transaction Network Services, Inc (TNS) is already fully integrated into the Aviation Department's parking system infrastructure, changing to a new vendor would require replacing the entire centralized management software, reconfiguring all customized alerting systems, and retraining personnel on the new equipment. This transition would result in significant costs, both in terms of finances and time. It is my recommendation that Gateway Services with TNS be procured as a Sole Source. Per Numbered Memorandum Sequence No. 24-01, Delegation of Approval and Award Authority dated July 8, 2024, Sole Brands may be approved by the Purchasing Manager if the award amount does not exceed the approved threshold (\$300,000).

Purchasing Agent Signature:

**SALUSTIO
JARAMILLO**

Digitally signed by SALUSTIO
JARAMILLO
Date: 2025.06.03 13:46:05 -04'00'

Reviewer Title:

Purchasing Manager

Reviewer Signature:

Jose Hidalgo

Digitally signed by Jose
Hidalgo
Date: 2025.06.03 14:22:49
-04'00'

APPROVAL AUTHORITY



APPROVED



DISAPPROVED

REASON/SUGGESTED ACTION (IF DISAPPROVED):

Title: Director of Purchasing

Signature: Constance Mangan,
Asst. Director, on behalf
of

Digitally signed by Constance
Mangan, Asst. Director, on behalf of
Date: 2025.06.03 15:35:02 -04'00'

PNC544999F1 - Transaction Network Services (TNS) Gateway Services

BPRO Electronic Procurement System [Back to list](#)



Project Details

Project: Transaction Network Services (TNS) Gateway Services

May 2025

prev next

Ref. #: PNC544999F1

Department: FASD - Purchasing

Type: RFI

Status: CLOSED

Open Date: May 2nd 2025, 4:30 PM EDT

Questions Due Date: May 16th 2025, 5:00 PM EDT

Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	28	29	30	1	2	3
					4:30p	OPEN
4	5	6	7	8	9	10
OPEN						
11	12	13	14	15	16	17
OPEN						
18	19	20	21	22	23	24
OPEN						
25	26	27	28	29	30	31

Contact Information: Lucho Jaramillo (Primary), Gerold Garrity (Alternate), sajaramillo@broward.org ggarrity@broward.org

Close Date: May 23rd 2025, 2:00 PM EDT

Days Left: Submissions are now closed

Contract Duration:
Not Applicable (RFQ/RFI)

Contract Renewal:
Not Applicable (RFQ/RFI)

Bid Validity:
Not Applicable

Bonding Required:
No

Total Amount of Pass-Thru Allowance (Initial Term or Fixed):
0

OESBD Designation Goal Participation Type (Multi):
No Goal

Goal Assigned Percentage (0 if No Goal):
0

Public Works/Construction:
No

Project Description:
Notice of Intent to Designate Sole Source/Sole Brand:

This Request for Information (RFI) Notice of Intent to Designate Sole Source to determine if the specified commodity or service is available from multiple providers, or if an alter commodity or service is available that would meet the County's needs. This is not a request for pricing or a purchase commitment.

The following commodity/service is thought to be available from only one sole source and is the only commodity/service that meets the County's needs for this Project:

Transaction Network Services, Inc. ("TNS") data services, software, software development and/or software support for operating ADVAM payment processing system/equipmen located at Broward County Aviation Department (BCAD). BCAD's new parking system includes ADVAM payment processing system (equipment); ADVAM only uses TNS's proprietary software.

This RFI will remain posted until closing date and time.

Prospective Vendors are requested to provide information regarding their ability to provide the commodity or service described or written explanation or other documentation contesting the proposed RFI designation.

If you are capable of meeting or exceeding the County's requirements for the specified commodity or service, respond to this RFI through the electronic bidding system. Vendor should upload any supporting information in the electronic bidding system as part of its response to assist the County in determining if commodity or service is comparable, is available from multiple suppliers, and meets the County's needs. The Director of Purchasing shall have sole authority in deciding what is comparable.

The Director of Purchasing shall consider such submittals and notify all submitting vendors (thru the electronic bidding system) of the decision whether to designate as a Sole Source/Brand, which decision shall not be subject to objection, protest, or appeal.

Important Events:

Search

PASSED	Open Date	Online Portal	Posting date for the Opportunity	May 2nd 2025, 4:30 PM EDT	N/A
PASSED	Questions Due Date	Online Portal	Deadline to submit Questions	May 16th 2025, 5:00 PM EDT	N/A
PASSED	Close Date	Online Portal	Deadline for Submissions	May 23rd 2025, 2:00 PM EDT	N/A

Commodity Codes:

- NIGP 94635 Credit Card, Charge Card Services
- NIGP 94670 Payment Card Services
- NIGP 94676 Smartcards, Limited and Standard Use Proximity Integrated Circuit Card (LU-PICC AND PICC)
- NIGP 6800226 CARD READER SYSTEM, ELECTRONIC, INCLUDING PARTS AND ACCESSORIES
- NIGP 9467020 ELECTRONIC PAYMENT TRANSFER

Requested Information:

Listed below are the documents and information needed to complete your submission:

--

Document Takers

Search

Vendors	# Files	Actions
No data available in table		

Interested Contractors

Search

Prime/General Contractors

Subcontractors

Search

Vendors	Contact	Email	Phone	Subcontract Services
No data available in table				

Messages

Public Notices (0)

Vendor Discussions (0)

Public Q&A (0)

There is currently nothing to display here.

Create a new Public Noti

Submissions and Prime/Subcontractor Interest

This project is not open for proposal submissions at this time.

SERVICE AGREEMENT

This Service Agreement (“Agreement”) is made as of May 30, 2025 (“Effective Date”) by and between Transaction Network Services, Inc. (“TNS”), having a principal place of business located at 10740 Parkridge Blvd., Suite 100, Reston, Virginia, 20191, and Broward County, a political subdivision of the State of Florida, having a principal place of business located at 320 Terminal Drive, Suite 200, Fort Lauderdale, Florida 33315 (“Customer,” “Client,” or “County”).

TNS and Customer agree that the following terms and conditions apply to the provision and use of the transaction-oriented data services, software, software development and/or software support provided by TNS under this Agreement (collectively “Services”) referenced in Service Schedule 1 and its exhibits and any additional attachments, schedules and addenda (each an “Attachment”) to this Agreement. Such attachments are an integral part of this Agreement. When used herein, the defined term “Agreement” shall include this Agreement and all Attachments. If there is a conflict between the terms of this Agreement and any Attachment, the terms of the Attachment shall prevail over the terms of this Agreement. Unless noted otherwise, the Services are to be used entirely within the United States.

In consideration of the foregoing and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties hereto agree as follows:

1. Term; Fiscal Year.

(a) The term (“Initial Term”) of this Agreement shall be for a period of thirty-six (36) months, commencing on the Effective Date, and may be renewed upon written approval of the County Purchasing Director, for up to two (2) additional terms of twelve (12) months each (each a “Renewal Term”) (the Initial Term and all Renewals Terms collectively the “Term”), unless (a) terminated sooner in accordance with the provisions herein, or (b) either party terminates this Agreement by giving written notice of termination to the other at least sixty (60) days prior to the effective date of any such Renewal Term; provided that this Agreement may not be renewed for the next Renewal Term if the total compensation projected to be paid by County to TNS would exceed an aggregate total under the Agreement of \$500,000.00.

(b) The continuation of this Agreement beyond the end of any County fiscal year (October 1 through September 30) is subject to both the appropriation and the availability of funds pursuant to Chapter 129 and, if applicable, Chapter 212, Florida Statutes.

2. Responsibilities.

(a) Customer is obtaining the Services under this Agreement for the purpose of payment card processing at Customer’s parking facilities at Fort Lauderdale-Hollywood International Airport (“Stated Purpose”), for which necessary equipment and software parking are provided, operated, and maintained by Customer’s contractor, Designa Access Corporation (“Designa”). Customer may subcontract its commitments, representations, or obligations of Customer stated in this Agreement to its contractor Designa, but Customer shall retain full responsibility for said commitments, representations or obligations that Customer subcontracts. All statements in this Agreement as to the respective obligations or responsibilities of Customer or TNS are statements solely as between Customer and TNS, and in no way modify the rights and obligations as between Customer and Designa pursuant to the Technology Products Agreement dated September 19, 2023.

(b) Customer and TNS shall comply with all applicable laws, regulations, industry codes of practice (“Applicable Law”) when providing or using the Services. Customer is solely responsible for the content of communications transmitted by Customer and/or its customers using the Services, and shall defend, indemnify, and hold harmless TNS (as defined in Paragraph 7(b)) from and against all liabilities and costs (including reasonable attorney’s fees) arising from any and all claims by any person based upon the content of any such communications.

(c) Customer shall ensure that all Customer-provided equipment that connects to the Services will perform according to published technical specifications for such equipment and TNS' interface specifications. Customer shall be responsible for the use and compatibility of equipment or software not provided by TNS. This Agreement does not include the provision, maintenance or repair by TNS of Customer-provided equipment or software, including, but not limited to, terminals, Customer's host computer and other non-TNS equipment or products.

(d) Customer is not permitted to resell, lease, sublicense or otherwise transfer all or any portion of the Services. If Customer permits third parties to access the Services, Customer shall defend, indemnify, and hold harmless TNS (as defined in Paragraph 7(b)) from and against all liabilities and costs (including reasonable attorney's fees) to the extent arising from any and all claims by any such third party in connection with the Services, regardless of the form of action, whether in contract, tort (including TNS' negligence), warranty, or strict liability. However, Customer's obligation to indemnify TNS under this section shall not apply to: (a) claims that arise from the violation of any federal, state or local law, regulation or ordinance by TNS, (b) claims that arise from a material breach of this Agreement by TNS, (c) indemnification under Section 6(c) herein or (d) claims for direct damages to real or tangible personal property, or for bodily injury or death proximately caused by TNS' negligence.

(e) Customer shall use the Services only for lawful purposes as well as in accordance with the terms and conditions set forth in the Attachments to this Agreement and in the documentation, manuals and policies provided by TNS. To the extent deemed necessary by Customer, Customer shall implement security procedures necessary to limit access to the Services to Customer's authorized users and shall maintain a procedure external to the Services for reconstruction of lost or altered files, data or programs.

(f) Customer agrees to reimburse TNS for reasonable documented out-of-pocket costs incurred by TNS for any equipment or services ordered by Customer but canceled before installation, for changes in delivery instructions, or for the relocation of TNS equipment at Customer's request.

(g) Customer agrees to provide TNS any assistance or cooperation it may reasonably request related to the Services. Customer also agrees to permit reasonable access to any Customer site by TNS employees or agents during normal business hours for the installation, servicing or removal of TNS equipment. Notwithstanding the foregoing, Customer agrees that TNS employees or agents shall have immediate access to any Customer site where TNS Equipment is located in the event of an emergency. TNS agrees that all such TNS employees or agents shall abide by Customer's rules and procedures, provided to TNS in writing, while on Customer's premises.

(h) Customer represents and warrants that: (i) the full legal name of the legal entity intended to receive the benefits and Services under this Agreement is accurately set forth herein; (ii) the person signing this Agreement has been duly authorized to execute this Agreement on Customer's behalf; and (iii) the execution hereof is not in conflict with any law, Customer's charter or bylaws, or any agreement to which the Customer is bound. TNS may act in reliance upon any instruction, instrument, or signature provided in writing by the County Contract Administrator or County Purchasing Director acting within their delegated authority under this Agreement, pursuant to Board delegation, or authorized by the Broward County Procurement Code, in connection with this Agreement.

3. Pricing.

(a) Prices for the Services are set forth in the Attachment(s) hereto. In connection with Services provided to Customer by TNS, Customer agrees to pay TNS the fees and charges relating to such Services set forth in such Attachment(s). Unless otherwise specified, all fees and charges are in U.S. Dollars and are exclusive of any applicable Taxes (as such term is defined in Paragraph 3(c) below), which, subject to Paragraph 4(c), will be separately stated and included on each monthly invoice. The prices also do not include, and TNS may impose (or pass through) additional fees and charges on Customer to recover, fees and charges imposed on the provision of the Services as a result of any Regulatory Activity (as such term is defined in Paragraph 3(c) below). Notwithstanding the foregoing, and subject to Paragraph 4(c), the County is exempt from federal and state taxes and shall not be liable for any such Taxes in connection with the Services provided by TNS under this Agreement provided Customer provides a valid tax exemption certificate.

(b) In the event there is a change in Customer's Service requirements that results in an increase in equipment provisioning, facility costs and/or scope of development or implementation, TNS reserves the right to change the prices for the Services to account for any such increase during any term of this Agreement. Customer acknowledges that tariffed charges (including, but not limited to, local access charges and call set-up charges), which are imposed by third party carriers and which may be passed through to Customer as set forth herein, are beyond the control of TNS and may be changed by such third party carriers at any time during the Term. To the extent that any such change results in a price increase that TNS elects to pass through to Customer during the Initial Term or any Renewal Term, TNS will furnish to Customer at Customer's request such materials as are reasonably necessary to document such increase.

(c) For purposes of this Agreement, "Taxes" means any and all applicable foreign, federal, state and local taxes, including without limitation all use, sales, value-added, surcharges, excise, franchise, property, commercial, gross receipts, license privilege or other similar taxes, levies, surcharges, duties, fees, or other tax-related charges, whether charged against Customer or TNS, with respect to the Services and any facilities provided by TNS, but excluding taxes imposed on TNS' revenues or net income. For purposes of this Agreement, "Regulatory Activity" means any regulation and/or ruling, including modifications thereto, by any governmental or quasi-governmental authority, including, without limitation, universal service fund programs (state and federal).

(d) TNS reserves the right to change the prices for Services provided to Customer by TNS upon sixty (60) days written notice to Customer at any time after the twenty-fourth (24th) month of the Initial Term, provided that any changes in the prices for Services will not exceed the lesser of three (3%) percent or the percentage change in the Consumer Price Index for All Urban Consumers as published by the United States Department of Labor (the "CPI-U") applicable at the time of TNS's notice of such change compared against the CPI-U for the same calendar month of the preceding year.

4. Billing and Payment.

(a) Customer shall pay TNS all charges as and when due under this Agreement, without deduction or setoff. Customer shall have the right to dispute any amount so invoiced and must notify TNS in writing of its dispute within sixty (60) days of the receipt of such invoice. A copy of the written notification of disputed charges plus any documentation supporting Customer's claim shall be forwarded to TNS at the address set forth in this Agreement. Any disputed charges resolved in favor of Customer shall be credited to Customer's account on the next invoice following resolution of the dispute. Any disputed amounts determined to be due and payable to TNS shall be due within fifteen (15) days of the resolution of the dispute.

(b) All payments shall be made through Electronic Funds Transfer (EFT) initiated by the Customer unless otherwise mutually agreed to in writing by the parties. TNS shall not initiate any direct debit from the Customer's account. All invoices are due in full and the Customer bears the cost of all bank fees associated with initiating payments to TNS. Bills will be issued monthly and are payable within thirty (30) days from the date shown on the invoice.

(c) Customer agrees to pay any Taxes due on the Services, unless Customer provides a valid tax exemption certificate. Should any federal, state or local jurisdiction determine that Taxes that have not been billed by TNS (and interest, penalty and/or surcharges thereon) are due on the provision of any Services provided under this Agreement, TNS shall so advise Customer and Customer shall be liable for any such Tax, interest, penalty and surcharge. Notwithstanding the foregoing, Customer shall not be liable for any penalty or surcharge to the extent it arises as a result of TNS' failure to properly and timely bill the taxes on which the penalty or surcharge is being assessed (unless such failure to bill is the result of an invalid tax exemption certificate supplied to TNS by Customer in which case Customer shall be responsible for the assessed penalty or surcharge). However, if the Customer disagrees with the assessment of any such additional Tax, penalty, surcharge and interest, the Customer shall, at its option and expense (including payment of any such assessment prior to final resolution of the issue), have the right to protest the

assessment and participate in any legal challenge to such assessment, but shall be liable for any Tax, penalty, surcharge and interest ultimately determined to be due. TNS shall, when requested by Customer and at Customer's expense, cooperate with Customer in any such protest or legal challenge.

(d) TNS agrees that Customer may audit TNS' books and records directly related to the Services provided to Customer under this Agreement no more than once a year at Customer's sole expense provided that Customer provides TNS with at least thirty (30) days advance written notice, and upon a time mutually agreed upon by the parties. In addition, Customer agrees to comply with TNS' security requirements and shall conduct any audit in a manner that does not unreasonably interfere with the ordinary business operations of TNS.

5. Termination.

(a) Except as otherwise provided herein, if Customer (i) fails to pay any outstanding charges within ten (10) days after receipt of written notice from TNS of delinquency, (ii) fails to perform or observe any other material term or condition of this Agreement within thirty (30) days after receipt of written notice from TNS of such failure, or (iii) files for protection under bankruptcy laws, makes an assignment for the benefit of creditors, appoints or suffers appointment of a receiver or trustee over its property, files a petition under the bankruptcy or insolvency act or has any such petition filed against it which is not discharged within sixty (60) days of the filing thereof, TNS may, at its discretion, suspend providing the Services and/or terminate this Agreement. If TNS terminates this Agreement, then Customer shall be liable for all charges incurred as of the date of termination. If TNS suspends providing the Services, then Customer shall be liable for all license fees or other recurring charges related to the suspended Services during the period of suspension.

(b) Except as otherwise provided herein, if TNS (i) fails to perform or observe any material term or condition of this Agreement within thirty (30) days after receipt of written notice from Customer of such failure, or (ii) files for protection under bankruptcy laws, makes an assignment for the benefit of creditors, appoints or suffers appointment of a receiver or trustee over its property, files a petition under any bankruptcy or insolvency act or has any such petition filed against it which is not discharged within sixty (60) days of the filing thereof, Customer may terminate this Agreement. In addition, Customer may terminate this Agreement at any time after the Initial Term, upon at least ninety (90) days written notice to TNS. If Customer terminates this Agreement pursuant to this Section 5(b), except for charges incurred as of the date of termination, Customer shall have no further financial obligations to TNS under this Agreement. Additionally, TNS shall reimburse the County, within ten (10) days after any such termination, any prepaid or unexpended funds paid by Customer but not due for Services rendered for time periods prior to the termination date.

(c) If Customer cancels or terminates this Agreement or the Services provided hereunder before the completion of the Initial Term or any Renewal Term for any reason whatsoever other than pursuant to Section 5(b) above, Customer agrees to pay TNS, within thirty (30) days of Customer's receipt of an invoice therefore from TNS any disconnection, early cancellation, termination or other charges paid by TNS to third parties that arises as a result of such cancellation or termination

6. Intellectual Property/License.

(a) As between Customer and TNS, Customer acknowledges that all Intellectual Property Rights (defined below) in the Services belong to and shall belong to TNS and, except as set forth in Section 6(b) below or in an applicable Attachment, Customer shall have no rights therein or thereto. "Intellectual Property Rights" means all intellectual property and rights to that property subsisting in any part of the world, whether or not registered, including all rights conferred by statute, common law or in equity in relation to: (i) inventions, patents and discoveries whether or not registered and improvements of products, technology, processes, methods or techniques; (ii) copyright (including future copyright) throughout the world in all literary works, artistic works, computer software, and any other works or subject matter in which copyright subsists and may in the future subsist; (iii) confidential information, trade secrets, technical data and know-how; (iv) designs, trade and service marks, business

names, trade names and logos; (v) any business name registration, domain name registration or social media account; (vi) any other rights resulting from an intellectual activity in the industrial, commercial, scientific, literary or artistic fields which subsist or may hereafter subsist; and (vii) any application or right to apply for registration of any of the above.

(b) TNS hereby grants to Customer a personal, nonexclusive, nontransferable license during the Term to use, in object code form, all software, manuals and other documentation ("Licensed Material") which may be furnished to Customer under this Agreement, provided such license shall automatically terminate upon expiration or termination of this Agreement. This license is limited to use in the United States and may not be transferred or sublicensed in any way except as permitted herein. Customer agrees to use its best efforts to ensure that its employees, and users of all Licensed Material hereunder comply with the terms and conditions set out in this Agreement. Customer also agrees to refrain from taking any steps, such as reverse assembly or reverse compilation, to derive a source code equivalent to the software. All Licensed Material furnished to Customer under this Agreement shall be used by Customer only to support Customer's use of the Services, shall not, without TNS' prior written consent, be reproduced or copied in whole or in part, shall not be removed from the United States, and shall be returned to TNS at the conclusion of the term of this Agreement.

(c) TNS shall defend, indemnify, and hold Customer harmless, at the expense of TNS, against any claims, actions or suits brought against Customer based on a claim of infringement of any United States patent or copyright arising out of use by Customer of the Services and/or the Licensed Material. TNS shall pay all costs, damages and expenses (including reasonable outside counsel attorney's fees) in any such suit, provided that (i) Customer provides prompt notice of any such claim, action or suit to TNS; (ii) TNS shall have total control of the defense of the claim, action or suit; and (iii) Customer reasonably cooperates in any such defense as reasonably requested by TNS. If a final injunction is obtained against TNS prohibiting the use by Customer of the Services and/or the Licensed Material due to infringement of a United States patent or copyright, TNS will, at its option, either (i) procure the right for the Customer to continue using the Services and/or the Licensed Material, or (ii) direct Customer to return any TNS materials in its possession relating to the infringing Services and/or Licensed Material at the expense of TNS. In the case of (ii), Customer will have the right to terminate this Agreement, and TNS will repay to Customer any charges paid to TNS in advance, prorated to the date of termination. Notwithstanding the above, TNS will have no obligation under this Paragraph 6(c) to the extent that: (1) any infringement is caused or contributed to by Customer, (2) Customer has combined, operated or used services, equipment or software not contemplated by this Agreement or any Attachment with any other devices or programs not authorized by TNS, or (3) Customer has modified Services or Licensed Material in a manner that has not been authorized in writing by TNS. This Paragraph 6(c) provides the sole and exclusive obligations and remedies of the parties in connection with any third-party claims, actions, suits, or other demands described in this Paragraph 6(c) or that otherwise asserts a violation of a third party's intellectual property rights.

7. Warranty and Limitation of Liability

(a) Under this Agreement, TNS provides services and related goods. TNS warrants that it will perform the Services in a workmanlike manner in accordance with applicable laws and regulations. Products, software or services sold or provided by TNS under this Agreement, are governed solely by the terms and conditions set forth in this Agreement and any applicable Attachments, including any warranties, guarantees, service level agreements or other obligations of TNS under such Attachments. Customer understands and agrees that the service credits, if any, set forth under such Attachments shall be Customer's sole remedy and the sole liability of TNS with respect to any failure by TNS to meet the performance standards set forth under the applicable Attachment, TNS makes no other warranty or guarantee, express or implied, under this Agreement, and TNS expressly disclaims any implied warranties of merchantability and fitness for a particular purpose.

(b) For purposes of this Paragraph 7(b), TNS includes TNS and any affiliated and subsidiary companies of TNS, and the directors, employees, officers, agents, subcontractors and suppliers of all of them.

(i) EXCEPT FOR TNS' INDEMNIFICATION OBLIGATIONS SET FORTH IN SECTION 6 (C) ABOVE FOR INTELLECTUAL PROPERTY INFRINGEMENT, TNS' LIABILITY TO CUSTOMER ON ACCOUNT OF ANY ACTS OR OMISSIONS RELATING TO THIS AGREEMENT SHALL BE LIMITED TO

PROVEN DIRECT DAMAGES IN AN AGGREGATE AMOUNT NOT TO EXCEED AN AMOUNT EQUAL TO THE AMOUNT PAID BY CUSTOMER TO TNS DURING THE SIX (6) MONTHS PRECEDING THE MONTH IN WHICH THE CAUSE OF ACTION AROSE. HOWEVER, NOTHING IN THIS SUBPARAGRAPH 7(b)(i) LIMITS TNS' LIABILITY FOR DIRECT DAMAGES TO REAL OR TANGIBLE PERSONAL PROPERTY, OR FOR BODILY INJURY OR DEATH, PROXIMATELY CAUSED BY TNS' GROSS NEGLIGENCE OR WILLFUL MISCONDUCT.

(ii) NEITHER TNS NOR CUSTOMER SHALL BE LIABLE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, RELIANCE, PUNITIVE OR SPECIAL DAMAGES, INCLUDING LIMITATION DAMAGES FOR HARM TO BUSINESS, LOST PROFITS, LOST SAVINGS OR LOST REVENUES, WHETHER OR NOT SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES; PROVIDED HOWEVER THAT NOTHING CONTAINED IN THIS CLAUSE (ii) SHALL LIMIT CUSTOMER'S LIABILITY TO PAY ANY CHARGES, FEES AND/OR AMOUNTS DUE HEREUNDER FOR SERVICES ACTUALLY PROVIDED BY TNS TO CUSTOMER PURSUANT TO THE TERMS HEREOF.

(iii) These limitations of liability shall apply regardless of the form of action, whether in contract, warranty, strict liability or tort, including without limitation negligence of any kind, whether active or passive, and shall survive failure of an exclusive remedy.

(iv) TNS shall not be liable for (A) service impairments caused by acts within the control of Customer, Customer's customers, employees, agents, subcontractors, suppliers or licensees or (B) interoperability of specific customer applications.

8. Confidentiality

(a) All tangible technical or business information, know-how, specifications, inventions, trade secrets, processes or Intellectual Property Rights that are of a confidential nature disclosed by one party to the other party shall be deemed the property of the disclosing party and shall be returned upon request. The receiving party shall: (i) keep such information in strict confidence; (ii) restrict disclosure of such information solely to its employees, consultants, advisors or subcontractors with a need to know and the employees, consultants, advisors or subcontractors of its affiliated companies with a need to know; and (iii) use the same degree of care as it uses for its own confidential information to prevent the unauthorized disclosure, use or publication of such proprietary information, which shall in any event be no less than a reasonable standard of care. The receiving party shall not use such information for any purpose other than to perform its obligations under this Agreement. The receiving party also shall ensure that its employees, consultants, advisors and subcontractors to whom it discloses such information comply with this Paragraph 8(a).

(b) The receiving party shall have no obligation to preserve the confidentiality of any information that: (i) was previously known to the receiving party or any of its affiliated companies free of any confidentiality obligation; (ii) is disclosed to third parties by the disclosing party without restrictions; (iii) becomes publicly available by means other than unauthorized disclosure; (iv) is independently developed by the receiving party; or (v) is required to be produced pursuant to Applicable Law.

(c) TNS Confidential Information. TNS represents that the Services include proprietary products and trade secrets of TNS. Accordingly, to the full extent permissible under Applicable Law, Customer agrees to treat intellectual property within the Services as confidential in accordance with this section. For any other material submitted to Customer, TNS must separately submit and conspicuously label as "RESTRICTED MATERIAL – DO NOT PRODUCE" any material (a) that TNS contends, constitutes, or contains its trade secrets under Chapter 688, Florida Statutes, or (b) for which TNS asserts a right to withhold from public disclosure as confidential or otherwise exempt from production under Florida public records laws (including Chapter 119, Florida Statutes) (collectively, "Restricted Material"). In addition, TNS must, simultaneous with the submission of any Restricted Material, provide a sworn affidavit from a person with personal knowledge attesting that the Restricted Material constitutes trade secrets or is otherwise exempt or confidential under Florida public records laws, including citing the applicable Florida statute and specifying the factual basis for each such claim. Upon request by County, TNS must promptly identify the specific applicable statutory section that protects any particular document. If a third

party submits a request to County for records designated by TNS as Restricted Material or for trade secret material in the Software or the Hosted Service, County shall refrain from disclosing such material unless otherwise ordered by a court of competent jurisdiction, authorized in writing by TNS, or the claimed exemption is waived. Any failure by TNS to strictly comply with the requirements of this section shall constitute TNS' waiver of County's obligation to treat the records as Restricted Material. TNS must indemnify and defend County and its employees and agents from any and all claims, causes of action, losses, fines, penalties, damages, judgments, and liabilities of any kind, including attorney's fees, litigation expenses, and court costs, relating to nondisclosure of Restricted Material or materials relating to the Software or the Hosted Service in response to a third-party request.

(d) County Confidential Information. All materials, data, transactions of all forms, financial information, documentation, inventions, designs, and methods that TNS obtains from County in connection with this Agreement, or in which County holds proprietary rights, constitute "County Confidential Information." All County-provided employee information, financial information, and personally identifiable information for individuals or entities interacting with County (including, without limitation, social security numbers, birth dates, banking and financial information, and other information deemed exempt or confidential under Applicable Law) also constitute "County Confidential Information."

1. County Confidential Information may not, without the prior written consent of County, or as otherwise required by Applicable Law, be used by TNS or its employees, agents, subcontractors or suppliers for any purpose other than for the benefit of County pursuant to this Agreement. Neither TNS nor its employees, agents, subcontractors, or suppliers may sell, transfer, publish, disclose, display, license, or otherwise make available to any other person or entity any County Confidential Information without the prior written consent of County.

2. TNS expressly agrees to be bound by and to defend, indemnify, and hold harmless County and its officers and employees from the breach of Applicable Law by TNS or its employees, agents, subcontractors, or suppliers regarding the unlawful use or disclosure of County Confidential Information.

3. Upon TNS' receipt of Customer's written request upon expiration or termination of this Agreement, or as otherwise demanded in writing by County, TNS shall use commercially reasonable efforts to turn over to County all County Confidential Information, in any form, tangible or intangible, possessed by TNS or its employees, agents, Subcontractors, or suppliers.

(e) TNS acknowledges that Customer is subject to Florida's public records laws, including Chapter 119, Florida Statutes, and agrees to comply with all applicable requirements related thereto. If TNS receives a request for public records regarding this Agreement or the Services, TNS must immediately notify the County's Contract Administrator in writing and provide all requested records to County to enable County to timely respond to the public records request. County will respond to all such public records requests. Any action taken by County in compliance with, or in a good faith attempt to comply with, the requirements of Chapter 119, Florida Statutes, shall not constitute a breach of this agreement.

(f) Maintenance of Confidential Information. Each party shall advise its employees, agents, subcontractors, and suppliers who receive or otherwise have access to the other Party's Confidential Information of their obligation to keep such information confidential, and shall promptly advise the other party in writing if it learns of any unauthorized use or disclosure of said Confidential Information. In addition, the parties agree to cooperate fully and provide all reasonable assistance to ensure the confidentiality of the other party's Confidential Information as described in this article.

(g) Data and Privacy. TNS shall comply with all applicable data and privacy laws and regulations, including without limitation Section 501.171, Florida Statutes in connection with providing TNS' services to Customer pursuant to this Agreement, and shall ensure that County data transmitted by TNS in connection with providing the Services to Customer pursuant to this Agreement is not transmitted outside the United States, with the exception of the UK, Australia, India and Malaysia. TNS shall not sell, market, publicize, distribute, or otherwise make available to any third party any personal identification information (as defined by Sections 501.171, Section 817.568, or Section 817.5685, Florida Statutes, as amended) that TNS may receive or otherwise have access to in connection

with this Agreement, unless expressly authorized in advance by County. If applicable and requested by County in writing, TNS shall provide cryptographic deletion of County data and formal attestation of data removal through standard database operations.

(h) The receiving party agrees that any violation of any provision of this Paragraph 8 shall cause immediate and irreparable harm to the disclosing party and, in such event, an injunction restraining the receiving party from such violation may be entered against it, in addition to any other relief available to the disclosing party.

(i) The obligations under this Section 8 shall survive termination of this Agreement and any Attachments.

9. General

(a) Customer and TNS shall make a good faith effort to settle any disputes that may arise with respect to the terms and conditions or any subject matter referred to in or governed by this Agreement within sixty (60) days from the date the dispute is first discussed between the parties. If such dispute cannot be so settled through each party's respective escalation procedures, then the parties may elect, by mutual written agreement, to proceed to mediation before an agreed-upon mediator or any other dispute resolution proceeding agreed upon by the parties' litigation.

(b) This Agreement shall not prevent TNS from entering into similar agreements with third parties, or from independently developing, using, selling or licensing materials, products or services which are similar to those provided under this Agreement. Also, nothing in this Agreement shall create or vest in Customer any right, title, or interest in the Services, Licensed Materials or Intellectual Property Rights, other than the right to use the Services and the Licensed Materials under the terms and conditions of this Agreement.

(c) TNS' performance obligations under this Agreement shall be solely to Customer and not to any third party. Other than as expressly set forth herein, this Agreement shall not be deemed to provide third parties with any remedy, claim, right of action, or other right.

(d) The parties agree to comply with the Payment Card Industry Data Security Standard ("PCI DSS") where applicable.

(e) Neither party shall have any liability for damages or delays due to fire, explosion, lightning, power surges or failures, strikes or labor disputes, water, acts of god, the elements, war, civil disturbances, acts of civil or military authorities or the public enemy, inability to secure products or transportation facilities, fuel or energy shortages, acts or omissions of communications carriers or suppliers, or other causes beyond its control whether or not similar to the foregoing (each a "Force Majeure Event"). The period of performance shall be extended to such extent as may be appropriate, not to exceed the period of delay, after the cause of the delay has been removed. If the condition that causes an excusable delay or failure to perform lasts longer than forty-five (45) days, either party may terminate the affected Attachments upon three (3) business days prior written notice. Except for fees for Services rendered under this Agreement, neither party shall have further financial obligation or liability for such termination.

(f) Neither party shall publish or use any advertising, sales promotions, press releases or other publicity which uses the other party's name, logo, trademarks or service marks without the prior written approval of the other party, which approval shall not be unreasonably withheld.

(g) This Agreement shall be governed by and construed in accordance with the laws of the Commonwealth of Virginia, without giving effect to the conflicts of laws principles thereof. Notwithstanding the foregoing, Florida law shall govern all matters relating to sovereign immunity or public records laws. If Customer is required to indemnify TNS pursuant to this Agreement, the limitations on tort liability under Section 768.28, Florida Statutes, shall be the applicable limitations for Customer's indemnification obligations, regardless of the nature or basis of the claim(s) being indemnified. Nothing in this Agreement shall be construed as a waiver of sovereign immunity or the limits of liability set forth in Section 768.28, Florida Statutes, as amended.

(h) Any assignment by either party of any right, obligation or duty, in whole or in part, or of any other interest hereunder, without the written consent of the other party, shall be void except assignments to a parent company, a wholly-owned subsidiary, or a wholly-owned subsidiary of a parent. All obligations and duties of any party under this Agreement shall be binding on all successors in interest and assigns of such party. TNS may subcontract any or all of the work to be performed by it under this Agreement, but shall retain full responsibility for the work that is subcontracted.

(i) All notices, requests, demands and other communications hereunder shall be in writing and shall be deemed to have been duly given delivered when sent by registered or certified mail, return receipt requested, or by reputable courier as evidenced by a delivery receipt, to each party's respective address as set forth in the Agreement. The parties may change the addresses on five (5) days prior written notice.

(j) It is expressly understood and agreed that neither party hereto is an employee, agent or legal representative of the other, and unless specifically authorized in writing to do so, may not incur any obligations on behalf of or in the name of the other. This Agreement does not create either a partnership or joint venture between TNS and Customer.

(k) If any portion of this Agreement is found to be invalid or unenforceable, the remaining portions shall remain in effect and the parties will begin negotiations for a replacement of the invalid or unenforceable portion.

(l) The expiration or termination of this Agreement shall not relieve either party hereto of those obligations that by their nature are intended to survive.

(m) Failure to enforce any right or remedy available under this Agreement shall not be construed to be a waiver of the right or remedy or any other right or remedy.

(n) This is the entire agreement between the parties with respect to the Services provided hereunder and it supersedes all prior agreements, proposals, representations, statements or understandings, whether written or oral, concerning the Services. No change, modification or waiver of any of the terms of this Agreement shall be binding unless included in a written agreement and signed by both parties.

(o) This Agreement may be executed in one or more counterparts, all of which (when executed and delivered) shall be considered one and the same Agreement and shall become effective when one or more counterparts have been signed by each party and delivered by each party to the other party, it being understood that both parties need not sign the same counterpart. Counterparts may be delivered by facsimile or other electronic transmission method (including .pdf) and any counterpart so delivered shall be deemed to have been duly and validly delivered and be valid and effective for all purposes.

(p) The terms "paragraph" and "section" are used interchangeably herein to refer to the applicable provision of this Agreement. Whenever reference is made to a section or paragraph of this Agreement, such reference is to the section or paragraph as a whole, including all subsections thereof, unless the reference is made to a particular subsection or subparagraph of such section or paragraph.

(q) Required Florida Provisions. Except to the extent sovereign immunity may be deemed waived by entering into this agreement, nothing herein is intended to serve as a waiver of sovereign immunity by County. TNS warrants and represents: it has not been charged with committing, there has been no determination that it committed, a "public entity crime" as defined by Section 287.133, Florida Statutes; it has not been placed on the "discriminatory vendor list" as provided in Section 287.134, Florida Statutes; it is not a "scrutinized company" pursuant to Sections 215.473 or 215.4725, Florida Statutes; it is not, and for the duration of the Agreement will not be, ineligible to contract with TNS on any of the grounds stated in Section 287.135, Florida Statutes; it is, and for the duration of the term will remain, in compliance with Section 286.101, Florida Statutes; it has registered with and use the E-Verify system maintained by the United States Department of Homeland Security to verify the work authorization status of all newly hired employees in compliance with the requirements of Section 448.095, Florida Statutes; it is not owned by the government of a foreign country of concern; the government of a foreign country of concern does not have a controlling interest in TNS; and it is not organized under the laws of and does not have its principal place of business in, a foreign country of concern. By signature below, TNS by its duly authorized representative declares

the foregoing under penalty of perjury in compliance with Section 287.138(4), Florida Statutes. By execution of this Agreement by the undersigned authorized representative of TNS, TNS hereby attests under penalty of perjury that TNS does not use coercion for labor or services, as such terms are defined in Section 787.06, Florida Statutes; under penalties of perjury, the undersigned authorized representative of TNS declares that they have read the foregoing statement and that the facts stated in it are true. To the extent applicable, the provisions of Section 119.0701, Florida Statutes, are incorporated as if fully restated herein.

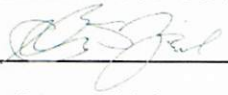
(r) Throughout the Term of the Agreement, TNS must maintain at least the minimum insurance coverage specified in Exhibit 6. All required policies must be issued by insurers with an A.M. Best rating of A- or better and a financial size category of Class VII or higher. TNS must include Broward County as an additional insured on all required policies as follows: "Broward County, Fort Lauderdale-Hollywood International Airport, 320 Terminal Drive, Suite 200, Fort Lauderdale, FL 33315." Proof of required insurance coverage must be provided at least annually to County. All coverage must remain active throughout the Term. TNS shall ensure that any subcontractors comply with these insurance requirements. TNS is responsible for all deductibles or self-insured retentions and waives any subrogation rights against Customer.

IF TNS HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO TNS' DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS AGREEMENT, CONTACT THE CUSTODIAN OF PUBLIC RECORDS AT (954) 359-6100, JAGARASSINO@BROWARD.ORG AND ALSO COPY CONTACTFLL@BROWARD.ORG, 320 TERMINAL DRIVE, SUITE 200, FORT LAUDERDALE, FLORIDA 33315.

Both parties hereto represent that they have read this Agreement in its entirety, understand it and agree to be bound by all the terms and conditions stated herein.

[THE REMAINDER OF THIS PAGE IS INTENTIONALLY LEFT BLANK]

Transaction Network Services, Inc. ("TNS")

By: 

Name: George Zirkei

Title: SVP, Americas

Date: May 29, 2025

TNS Contact Person:

Jeff Otterstrom

Phone Number: _____

E-Mail jotterstrom@tnsi.com

Copy of Notices to:

Transaction Network Services, Inc.

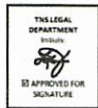
ATTN: Contract Administration

10740 Parkridge Blvd., Suite 100

Reston, Virginia, 20191

Phone: (360) 493-6000

Fax: (360) 493-6233 or contractadmin@tnsi.com



Broward County ("Customer")

Constance Mangan, Digitally signed by Constance
Asst. Director, on Mangan, Asst. Director, on behalf
of
By: behalf of Date: 2025.06.03 15:33:46 -04'00'

Name: Robert Gleason

Title: Purchasing Director

Date: _____

Customer Contact Person:

James Bryant Walker

Phone Number: 954-359-6475

E-Mail jamwalker@broward.org

Copy of Notices to:

Broward County Director of Aviation

320 Terminal Drive, Suite 200

Fort Lauderdale, Florida 33315

Email address: mgale@broward.org

Approved as to form by

Andrew J. Meyers

Broward County Attorney

115 South Andrews Avenue, Suite 423

Fort Lauderdale, Florida 33301

Telephone: (954) 357-7600

Digitally signed by Jessica
Alvarez
Date: 2025.05.30 11:12:35
-04'00'

By Jessica Alvarez (Date)

Jessica Alvarez
Assistant County Attorney

Digitally signed by Rene D. Harrod
DN: cn=Rene D. Harrod, ou=Broward
County Attorney's Office,

Reason: Approved as to form
Date: 2025.05.30 12:47:55 -04'00'

By  (Date)
René D. Harrod
Chief Deputy County Attorney

SERVICE SCHEDULE 1

UNATTENDED PAYMENT GATEWAY SERVICE

When used herein, the defined term “Service Schedule” shall include this Service Schedule and the following exhibits:

- Exhibit 1 – Defined Terms
- Exhibit 2 – Fees & Charges
- Exhibit 3 – Terms & Conditions
- Exhibit 4 – Service Levels
- Exhibit 5 – P2PE Instruction Manual
- Exhibit 6 – Certificate of Insurance

SECTION I – SERVICE SCHEDULE TERM

- A. The term of this Service Schedule will commence on the Commencement Date and will continue for the period set forth in Exhibit 2, unless terminated sooner as provided under this Service Schedule and/or the Agreement (“Service Schedule Initial Term”).
- B. The term of this Service Schedule may renew, at County’s option upon written notice by the County Purchasing Director, for up to two (2) additional terms of twelve (12) months each (each a “Service Schedule Renewal Term”), unless either party terminates this Service Schedule by giving written notice of termination to the other party at least sixty (60) days prior to the effective date of any such Service Schedule Renewal Term.

SECTION II – DESCRIPTION OF THE SERVICES

TNS will provide Client a gateway service that enables Client to transmit Transactions to financial institutions or payment processors (the “Services”). As part of Services TNS will provide:

- (i) a terminal software application, which integrates to the TNS gateway using defined messages to provide the payment card details to be processed; and
- (ii) terminal monitoring and support software maintenance services, such as inactive notifications and compliance maintenance of terminals connected to the Services.

The parties wish to record the terms of their agreement and understanding for:

- (i) TNS to provide consulting and other services to the Client as may be authorized from time to time;
- (ii) TNS to process card transactions for the Term of this Service Schedule.

EXHIBIT 1 TO SERVICE SCHEDULE

DEFINITIONS IN THIS SERVICE SCHEDULE UNLESS THE CONTEXT OTHERWISE REQUIRES:

“After Hours Support Fee” A fee charged for support requests that occur outside of TNS’ Standard Support Hours per the Service Levels set forth in Exhibit 4.

“Accounts Payable Email” means the Accounts Payable Contact Email address specified in this Service Schedule.

“Client” The Company, Individual or Commercial Entity for which TNS makes this Agreement with as set forth in Exhibit 2.

“Clients Payment Account” means the account nominated in Exhibit 2 of this Service Schedule (or as subsequently notified by the Client to TNS) as the account to which amounts payable to the Client, or to which amounts may be debited or adjusted as a result of transacting through TNS are to be credited, debited and adjusted.

“Business Day” means a day other than a Saturday, Sunday or public, special or bank holiday in the United States.

“Card Holder” means a person with a credit card, debit card or other means of electronic payment who attempts to enter into, or enters into, a Transaction with the Client by use of the Services.

“Commencement Date” means the date specified in Exhibit 2 of this Service Schedule.

“Consultancy Rate” The agreed rate of consultancy for any hourly services such as Project Management, Development, Quality Assurance and other activities as specified in Exhibit 2 of this Service Schedule.

“Fee” means all fees and charges payable by the Client in accordance with this Service Schedule.

“Hardware” means any physical hardware terminals, pin pads and card readers supplied by a third party and used by Client in connection with the Services.

“P2PE” Point-to-point encryption of cardholder data.

“P2PE Solution” A combination of secure devices, applications and processes that encrypt cardholder data from a PCI approved point of interaction (POI) device through to decryption.

“Personal Data” may include contact name, phone number, email or postal address. For definitions relating to a specific geography, refer to local Data Privacy regulations.

“Payment Card Data” means card data and track data including PAN, Expiry and where applicable CVV.

“Payment System” means the system whereby the **Client** can request, and TNS arranges, payments by Card Holders to the **Client** using the secure electronic payment service provided by TNS.

“PIM” An instruction manual attached hereto as Exhibit 5, which was prepared by the P2PE Solution Provider in accordance with P2PE Standard to instruct its customers and resellers/integrators on secure P2PE Solution implementation, to document secure configuration specifics and to clearly delineate vendor, reseller/integrator and customer responsibilities for installing and or using P2PE Solutions.

“POI” and “POI Device” means Point of Interaction and consists of hardware and software which is hosted in Client’s equipment to enable a Card Holder to perform a card transaction.

“Services” means the services as described in Section I of this Service Schedule.

“Service Level Agreement” means the service levels outlined in Exhibit 4.

“Sponsor” means the financial institution that sponsors TNS’ participation in the Bulk Electronic Clearing System for the purposes of TNS’ processing of Electronic Transactions.

“Term” is the period specified in this Service Agreement Schedule (subject to any earlier termination or extension in both cases in accordance with the terms set forth herein and the terms set forth in the Agreement).

“Transaction” means any Card Holder transaction type, including but not limited to Approved, Declined, Payments, Pre-Authorisations, Completions, Refunds and Reversals.

“Transaction Fee” A fee charged to Client for every Transaction received by the TNS gateway as specified in Exhibit 2. Each month TNS will bill Client an aggregate Transaction Fee calculated by multiplying the total number of Transactions in such month by the applicable per Transaction Fee.

**EXHIBIT 2 TO SERVICE SCHEDULE
FEES AND CHARGES**

Company Name:	Broward County
Registered Trading Name	Broward County Aviation Department
Business Type –	Government – Airport
	If Other, please specify:
Website address	www.broward.org; www.fll.net
Main Phone Number	(954) 359-0200
Accounts Payable Email	kruus@broward.org

Billing Address 320 Terminal Drive, Suite 200
Fort Lauderdale, FL 33315

Shipping Address	same	
-------------------------	------	--

All fees set forth in this table are applicable to Broward County and are in US dollars.**

Item	Fee	Billing Recurrence	Chargeable
Transaction Fee*	\$0.06	Monthly	Per Transaction
After Hours Support Fee	\$200.00	Upon completion of services	Per Request
Consultancy Rate	\$200.00	Upon completion of services	Per Hour

Commencement Date	May 30,	2025
Service Schedule Initial Term	36	Months

*Invoiced in arrears

** Client understands and agrees that the pricing set forth in this table is applicable to Broward County. Pricing for other Client third parties shall be mutually agreed upon by the parties and reflected in an amendment to this Service Schedule.

EXHIBIT 3 TO SERVICE SCHEDULE

TERMS AND CONDITIONS

1. MAINTENANCE AND SUPPORT

The Client appoints TNS to provide the Services to the Client in accordance with the terms of this Service Schedule and the Agreement.

TNS shall provide maintenance and support services to the Client in accordance with Exhibit 4 hereto.

The Client will designate for the Primary Support Site a single person to be the Support Contact and a backup Support Contact (together, the "Support Contact") who will liaise between the Client and TNS for matters related to the Maintenance and Support of the Service and the Client will use its best endeavors to ensure that only the Support Contact liaises with TNS regarding such matters.

Upon notification from the Support Contact (or if that person is not available, some other person in their place) of:

- 1.1.1. a request for support;
- 1.1.2. a failure of the Services to perform correctly; or
- 1.1.3. a request for an enhancement to the Services;

TNS will, within a period specified in the service levels in Exhibit 4 to this Service Schedule, use its best endeavors to provide the required response.

TNS shall comply with the service levels in Exhibit 4 of this Service Schedule.

The Support Services shall be provided per Exhibit 4 of this Service Schedule.

If agreed between TNS and the Client, TNS will provide onsite Support Services at the Primary Support Site during Business Hours of the Client at the Onsite Support Fee rate specified in the Exhibit 2.

Support Services will be provided by TNS, as agreed between TNS and the Client, outside the Business Hours at rates set out in Exhibit 2 for After Hours Support Fee.

Where the Client requests Support Services from TNS and TNS determines, after appropriate investigation, that the problem is not caused by the Services or the subject matter does not involve the Services, then TNS shall be entitled to charge the Client the External Issue Call Out Fee as specified in Exhibit 2 plus time spent on the support request at the following rates:

- 1.1.4. Where the support request is received during Business Hours, the External Issue Support Fee as set out in Exhibit 2 shall apply.
- 1.1.5. Where the support request is received outside Business Hours, the After-Hours Support Fee as set out in Exhibit 2 shall apply.

2. SUSPENSION/TERMINATION

TNS may immediately suspend the provision of the whole or any part of the Services until further notice on written or oral notice to the Client if:

- 2.1.1. TNS:

- 2.1.1.1. is entitled to terminate this Service Schedule and/or the Agreement;
 - 2.1.1.2. is requested to suspend by government or other competent authority;
 - 2.1.1.3. for any bona fide reason considers it necessary to do so, including without limitation, if the Client has breached any of its obligations;
- 2.1.2. TNS' Sponsor terminates or suspends its sponsorship arrangement with TNS;
- 2.1.3. the Client fails to maintain any necessary Client or third-party agreement in connection with Client's use of the Services as contemplated herein.

Nothing in clause 2.1 limits the Client's rights or remedies against TNS in circumstances where TNS's breach of agreement, fault, negligence or omission caused or contributed to the relevant suspension of the Services.

The Client is not entitled to any credit or refund of fees in respect of any period during which access to any Services is suspended due to the Client's breach, fault, negligence or omission.

If TNS suspends the Services due to the Client's breach, fault, negligence or omission and TNS subsequently agrees to reconnect the Services, the Client must reimburse TNS all reasonable costs and expenses incurred in suspending and recommencing the Services.

COPYING

The Client cannot make copies of any software supplied or provided by TNS.

3. INTELLECTUAL PROPERTY

Client understands that the services set forth herein are not exclusive to Client. Client also understands and agrees that TNS owns any and all intellectual property rights in relation to any and all of the Services provided to Client under this Service Schedule. Client agrees that TNS retains ownership of all intellectual property rights in the Services (including any associated software and documentation) as well as any modifications thereto, and Client shall have no rights therein or thereto other than the right to use them in accordance with the terms of this Service Schedule and the Agreement.

The Client will not reverse assemble, reverse compile or create source code from any software Client accesses through the Services.

The Client must immediately notify TNS in writing of any actual, suspected or anticipated infringement of TNS' intellectual property rights that comes to the Client's attention.

The Client agrees to provide reasonable assistance to TNS, at no cost to Client, with any enforcement of TNS' intellectual property rights.

4. THIRD-PARTY SOFTWARE

TNS shall use its reasonable endeavors to assist the Client to support third-party software, but shall not be responsible for support of the third-party software (other than third-party software required by or provided as

part of the Services) or operating system software of Client (collectively “Third-Party Software”) and will not be responsible for any deficiencies in such software, such responsibility falls solely on the Client .

TNS will not be liable for loss or damage suffered by the Client arising out of a deficiency or change in any Third-Party Software or a breach by the third party of its obligations under the applicable Third-Party Software license.

5. CLIENT OBLIGATIONS

The Client will:

- 5.1.1. subject to the Client’s confidentiality requirements, provide TNS with access to all relevant information, documents, computer systems and data and any other material which is necessary to allow TNS to perform the Services;
- 5.1.2. provide TNS or arrange for TNS to receive in a timely manner documentation and software in regards to the integration components and facilities provided by any third-party systems;
- 5.1.3. provide, in a timely manner, any information reasonably required by TNS in order to fulfill TNS’ obligations under this Service Schedule;
- 5.1.4. comply with TNS’ reasonable directions regarding, making or remedying any adjustments, errors, corrections, reversals, mistaken payments, overpayments, underpayments, unauthorized payments and fraudulent payments arising from or in connection with the use of the Services;
- 5.1.5. keep secure and not disclose to any other person passwords, encryption keys and all other codes provided by TNS for use in relation to the Services and exercise reasonable care and skill in the use, operation, protection, access to and security of any computer or other device used in connection with the Services;
- 5.1.6. monitor and reconcile their Service and payments, notifying TNS within 45 days of the date of the suspected discrepancy;
- 5.1.7. notify TNS immediately of any malfunction or breakdown of any Services;
- 5.1.8. not directly solicit or intentionally seek to engage the services of personnel provided by TNS under this Service Schedule either during or for a period of six (6) months after the termination of this Service Schedule without the written consent of TNS; for clarity, Customer’s routine public notice and posting of open positions and normal processes to review applications received and fill those positions is not a violation of this provision;
- 5.1.9. comply with all applicable data protection and/or privacy statutes, legislation and regulations.
- 5.1.10. comply with the provided P2PE Instruction Manual (PIM) if applying the TNS P2PE Solution, by implementing and maintaining all P2PE controls responsible for;
- 5.1.11. comply with TNS’ reasonable directions regarding making or remedying any adjustments, errors, corrections, reversals, mistaken payments, overpayments, underpayments, unauthorised payments or fraudulent payments arising from or in connection with the use of the Services;
- 5.1.12. maintain inventory-control and monitoring procedures to accurately track POI devices in their possession;

- 5.1.13. physically secure POI devices awaiting deployment or otherwise not in use;
- 5.1.14. implement procedures to prevent and detect the unauthorised alteration or replacement of POI devices in possession during deployment;
- 5.1.15. ensure that POI devices are physically secured or otherwise controlled to prevent unauthorised access, modification, or substitution while devices are deployed for use;
- 5.1.16. ensure that, POI devices maintain conformance with the corresponding Terminal Manufacturers Security Policy, including PIN shield installed, where deemed necessary for visual privacy.
- 5.1.17. prevent unauthorised physical access to devices undergoing repair or maintenance while in their possession.
- 5.1.18. complete regular inspection of the devices to prevent card information theft such as ‘card skimmers’ (magstripe readers) and ‘card shimmers’ (EMV Chip readers);
- 5.1.19. securely maintain POI devices being returned, replaced, or disposed of, and provide related instructions to third-party providers performing this service;
- 5.1.20. define and implement Card Scheme procedures for merchants on detecting and reporting tampered POI devices, including missing devices;
- 5.1.21. implement mechanisms to monitor and respond to suspicious activity on POI devices deployed at the Client location;
- 5.1.22. provide computer software, hardware and ancillary equipment reasonably specified by TNS which will effectively run the Services at the Client’s site/s (or other such site/s nominated by the Client as the Client’s site) and, where appropriate, access a Payment System;
- 5.1.23. monitor and reconcile their service and payments, notifying TNS within 45 days of the date of the suspected discrepancy.

VARIATION OF SERVICES

TNS may, with prior written notice to the Client, change the Services in order to comply with any applicable safety, regulatory, security, PCI-DSS or statutory requirements otherwise in any way which does not have a material adverse effect on the Client’s business operations or increase Client’s fees set forth herein.

TNS shall not be liable for violation of this Agreement to the extent of changes made to the provision of the Services where necessary to avoid or resolve third-party claims of intellectual property infringement with regard to the Services provided that TNS shall notify the Client promptly of any such changes as it becomes aware of them and shall use commercially reasonable means to maintain and provide the Services or substantially equivalent Services in compliance and consistent with the intent and purpose of this Agreement, and if requested by the Client shall facilitate and assist in any discussions between the Client and such third party in respect of such changes.

If either party requests a change to the scope or execution of the Services, TNS shall, within a reasonable time, provide a written estimate to Client of:

- 5.1.24. The likely time required to implement the change;
- 5.1.25. any variations to the Transaction Fees arising from the change; and

5.1.26. any other impact of the change on the terms of this agreement.

If either party request a change to the scope of the Services necessary to effectuate the purposes of this Agreement, the other party shall not unreasonably withhold or delay its consent to it.

If the Client wishes TNS to proceed with a material change, the parties will use their respective best endeavors to agree in writing necessary variations to its charges and any other relevant terms of this agreement to take into account the change.

No variation of this agreement shall be valid unless it is in writing and signed by or on behalf of each of the parties.

6. SPECIAL CONDITIONS

The Client acknowledges that the internet is not owned or controlled by TNS and TNS does not guarantee that its Services will be available at all times. TNS will at all times maintain its PCI DSS certification but is not responsible for security of the Client's information, data, text, files links, software, communication or other materials transmitted or received by the Services but not stored within the Services, which is solely at the Client's risk.

TNS agrees to comply with the Payment Card Industry Data Security Standard ("PCI DSS") where applicable. Upon receipt of County's written request, but no more than once per year, TNS shall provide to County:

- A copy of their Annual PCI DSS Attestation of Compliance ("AOC");

Except as otherwise expressly stated herein: TNS shall not be liable to the Client for any defects, loss or damage resulting from any improper use of any materials delivered by TNS to the Client under this Service Schedule. TNS Services are provided "as is", as available and with all faults, TNS does not warrant that the Services will meet all of the Client's requirements or that provision of the Services will be uninterrupted, error free or free from defects.

7. EFFECT OF TERMINATION

- 11.1 Any termination of this Service Schedule and/or the Agreement shall not affect any accrued rights or liabilities of either party, nor shall it affect any provision of this Service Schedule and/or the Agreement which is expressly or by implication intended to continue in force after such termination.
- 11.2 Immediately upon termination of this Service Schedule and/or the Agreement by TNS, the Client shall cease to use the Services.
- 11.3 In the event that this Service Schedule is terminated by the Client as a result of a breach by TNS pursuant to the terms set forth in Section 4(b) of the Agreement, then TNS shall refund any payments made by the Client for Services that have not been rendered.

EXHIBIT 4 TO SERVICE SCHEDULE SERVICE LEVELS

1.0 Support Levels and Hours of Provision

This Service Level Agreement does not apply to Hardware and the repair to, or replacement of, Hardware which is covered by TNS' Standard Terms and Conditions of Sale.

Standard Support hours are 08:30 – 17:30 Eastern Time, Monday to Friday excluding public holidays.

2.0 Issues Identified by TNS

Once an issue has been identified and diagnosed, TNS will send notification by email to the appointed Support and Technical Contacts of affected Clients.

3.0 Severity and Resolution

TNS commits to restoring core functionality within the times outlined below for each of the indicated time periods. Resolution times are measured from the time at which TNS first becomes aware of an issue.

Service Levels

1. Priority Level Definitions

Priority	Description	Examples
Severity Level 1 (P1)	There is: • a critical level of impact on the Services or on its end users; and/or • a system down situation in which no operation can continue; and/or • a critical function that is not available or is not functioning correctly and no work around is known.	• System crashes and fails to restart. • Failure to interact at all or correctly with any key internal or external interfaces. • Unable to make a payment from one or more channels.
Severity Level 2 (P2)	There is, or there is reasonably likely to be: • a serious (but not critical) level of impact on the Services or on its end users; and/or • a loss of service in which the operation of the Services continues in a restricted manner; and/or • malfunctioning of the Services, but it is still usable and partially inoperative, and the inoperative portion has a less critical impact on operations than Severity Level	• A fault is discovered causing limited usability of the Services.

Severity Level 3 (P3)	There is, or there is reasonably likely to be: • a moderate level of impact on the Services or on its end users; and/or • a limited loss of service/functionality resulting in minimal or no impact on the operation/application of the Services, that is not otherwise prioritised as critical or serious.	• A fault is discovered causing limited usability of the Services.
-----------------------	---	--

TNS will allocate a priority to a fault notified to TNS in accordance with the priority levels set out above.

Faults

Notification	The County must notify TNS upon becoming aware of any Fault, detailing the Fault.
Response	TNS will endeavour to respond to the County to discuss the Fault: a. in the case of a P1, within 1 hour of receipt of notification; or b. in the case of a P2 Fault notified within Support Hours, within 1 hour of receipt of notification; or c. in the case of a P2 Fault notified outside Support Hours or any P3 Fault, by 9:30 am the next Business Day but a call may be logged with TNS outside Support Hours.

Progress reports	TNS will endeavour to provide the Client with an update on the progress of resolution of the Fault: a. in the case of a P1 or P2 Fault b. within 1 hour after the response provided above; and c. then every 2 hours; and d. in the case of a P3 Fault e. within 1 hour after the response provided above; and f. then every 48 hours during Support Hours.
------------------	---

2. Maintenance

Scheduled Outage	TNS will give a minimum of 48 hours' notice to the Client's nominated Support Contact unless urgent maintenance is required to ensure continuity of the Services.
Emergency Outage	This is a situation in which urgent maintenance is required and TNS is unable to give 48 hours' notice. In this case, the Client's nominated contact person will be notified as early as practical prior to the time of the Emergency Outage.
Duration and timing	TNS will aim to keep the duration of maintenance under two hours.

3. Unscheduled Outages

Notification by the Certified Payment Gateway	Unless TNS has already provided notification to the Client of an Unscheduled Outage, the Client must notify the TNS helpdesk upon becoming aware of any Unscheduled Outage, specifying that an Unscheduled Outage has occurred and detailing the Unscheduled Outage.
Response Time	TNS will endeavour to respond to the Client to discuss the Unscheduled Outage: a. in the case of an Unscheduled Outage notified within Support Hours, within 1 hour of receipt of notification; or b. in the case of an Unscheduled Outage notified outside Support Hours, within 3 hours of receipt of notification.

Notification by TNS and updates	The Client to be first notified within 1 hour of TNS becoming aware of the Unscheduled Outage (by telephone or email during Support Hours and by email outside Support Hours) then updated periodically until system restoration.
---------------------------------	---

4.0 Chargeable Support

Support requested beyond the service level commitments in this Service Level Agreement will be charged in accordance with the Hourly Consultancy Rate. This includes but is not restricted to assistance in the resolution of issues that are not within TNS’ areas of responsibility.

Prior to the commencement of any chargeable work, the Client will be notified and TNS will await an affirmative response to the offer to proceed.

5.0 Service Commitment

An outage is defined as the unavailability or malfunction of the Services.

The duration of an outage will be measured as the time between when TNS becomes aware of an outage and the resumption of service provision following the implementation of a solution or suitable workaround. The Service availability (“**Service Availability**”) is calculated as the inverse of the duration of all outages during a period.

The measure of Service Availability discounts any contributing factors external to TNS or events or circumstances that are unforeseen or not otherwise within TNS’ reasonable control such as third-party provisioning failures.

TNS is committed to providing a premium level of Client service and a proactive approach to issue resolution, and will maintain a core Service Availability in excess of 99% over a rolling three-month period.

If over this period a 99% availability is not maintained, TNS shall pay Client the amount of the below for each month in which the rolling three-month period for the prior three months did not meet or exceed the Service Availability stated.

The following formula will be used to calculate the service level of the Service monthly:



$$\text{Monthly Availability} = \frac{\text{Total Production Minutes} - \text{Total Production Outage Minutes}}{\text{Total Minutes}} * 100$$

In the event TNS fails to maintain the service level target of 99.00% as defined herein in a given month, Customer may request a credit in such month based on the amounts in the table below

Monthly Availability	Eligible Service Credit Amount as % of Total Fees Paid to TNS per Month
Greater than or equal to 99.0%	0%
98.0% to 99.0%	10%
97.0% to 98.0%	20%
97.0% or less	30%

For purposes of this SLA, the term “Production Outage” means the period of time (measured in minutes) during which the operation of the TNS Service is impaired such that Customer cannot process online transactions. A Production Outage does not include periods of time during which the TNS Service is unavailable as a result of or due to (1) scheduled maintenance that Customer was advised of, in writing, at least five (5) business days prior to such scheduled maintenance, (2) force majeure events, (3) outages, failures or interruptions not within the TNS Network and control, or (4) the acts, negligence or willful misconduct of Customer, Customer’s customers, or the employees, agents, contractors, or service providers of Customer.

Customer understands and agrees that the Service Credits set forth in the above shall be Customer’s sole remedy and the sole liability of TNS with respect to any failure by TNS to meet the performance standards under this SLA. In addition, Customer understands and agrees that the terms and conditions set forth in this Section 5 apply only to the TNS Pay Unattended Payment Gateway Service.

For the avoidance of doubt, TNS only will apply credits against amounts it is owed by Customer under the Agreement. Credits for verified claims shall be applied to the next invoice sent to Customer after completion of verification. In no event may the total credits in any month for the TNS Unattended Gateway Service exceed the charges for such Service in the applicable month.

6.0 Scheduled Maintenance

To maximize optimal performance of the servers, TNS performs routine maintenance on the servers on a regular basis requiring servers to be temporarily taken offline.

TNS reserves four hours of server unavailability per month for maintenance purposes. This server unavailability will not be included in Service Availability calculations.

The maintenance is typically performed during off-peak hours, and TNS will provide advance notice of maintenance whenever possible.

7.0 Consulting

New work or modifications to existing Services can be commissioned by the Client contacting TNS with a detailed description of the objectives and requirements.

Where possible, TNS will work with all stakeholders to design and plan a viable solution, the costing of which will be presented to the Client as either a quote or a proposal.

8.0 Exclusions

The following exclusions shall apply when measuring any aspect of the Service Availability:

- a. Denial of service attacks or other types of attacks directed toward the infrastructure that supports the Services resulting in or contributing to downtime.
- b. Any type of outage or service degradation relating to unavailability of a financial institution including but not limited to issuers and/or acquirers or any other third-party switch or processing system.
- c. Any issues limited solely to the Client that cannot be proven against any other Client.
- d. Any failure or service outage that falls outside of TNS' reasonable control.
- e. Any act or omission of TNS in compliance with this Agreement, any law or any direction from a regulator or other government agency.
- f. Any act or omission of the Client which impacts Service Availability.

9.0 Client Contacts

- a. The Client must nominate a Sales, Support, Technical, Accounts Payable and Purchasing Contact when signing an Agreement and should they fail to nominate a Support Contact or Technical Contact or if the Support or Technical Contact leaves the company, the Sales Contact will become the Support or Technical Contact by default, unless they nominate a new Support or Technical contact by contacting the TNS Support team.
- b. TNS will automatically subscribe the following contacts to TNS Notifications. The contact is able to unsubscribe, where allowed, via [the TNS Preference Centre](#).
- c. The County is aware that the Support and Technical contacts cannot unsubscribe from support notifications (maintenance schedules etc).
- d. One person can be more than one Contact Type

Contact Type	Definition	Default Subscription	Mandatory Subscription
Sales Contact	Person who is the principal contact for the agreement. Owns the commercial relationship from the County's side	Event Updates TNS Newsletter Product Updates	
Project Contact	Person who is the principal day to day contact	Event Updates TNS Newsletter Product Updates	
Support Contact	Person who is responsible for the ongoing maintenance and availability of the service	Support Notifications TNS Newsletter	Support Notification
Technical Contact	Person who is responsible for completing technical implementation and changes to the service	Technical Notifications Support Notifications TNS Newsletter	Technical Notification Support Notification
Accounts Payable Contact	Person who is responsible for payment	N/A	N/A
Purchasing Contact	Person who is responsible for providing Purchase Order information	N/A	N/A
Security Contact	Person who is contacted in the event of a security incident	N/A	N/A

10.0 TNS Service, Support and Escalation

All service, support and escalation requests should be directed to:

Email: advam-support-us@tnsi.com

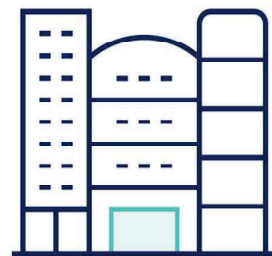
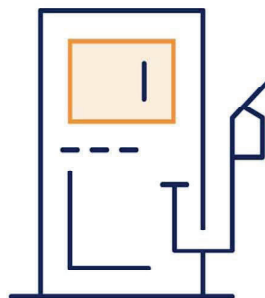
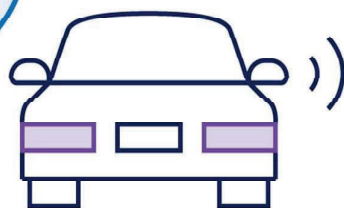
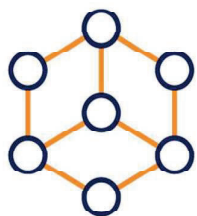
Phone: To be provided by TNS

**EXHIBIT 5 TO SERVICE SCHEDULE
P2PE INSTRUCTION MANUAL (“PIM”)**



ADVAM P2PE Instruction Manual

Version 3.3



ADVAM Pty Ltd is a wholly owned subsidiary of Transaction Network Services (TNS).

This document is the TNS P2PE Instruction Manual for the P2PE solution listed with PCI as “ADVAM P2PE Solution”. For the Purposed of this document the solution provider entity will be referred to as “ADVAM”.

This ADVAM P2PE Instruction Manual forms part of the Unattended Documentation or Documentation in respect of any terminal equipment supplied by ADVAM and is subject to the terms and conditions of the Services Agreement or Reseller Agreement (as the case may be) between ADVAM and the customer.

The information contained in this document is confidential and proprietary to ADVAM Pty Ltd. ADVAM submits this document with the understanding that it will be held in strict confidence and will not be disclosed, duplicated or used in whole or in part for any purpose other than the evaluation of ADVAM’s qualifications without the prior written consent of ADVAM.

For the purposes of Freedom of Information legislation, ADVAM classified this document as “Commercial-in-Confidence”.

Trademarks

Product names mentioned in this guide may be trademarks of their respective owners.

Revision History

Version Number	Revision Date	Revision Description
Draft 0.1	October 2018	Initial Draft release
Draft 0.2	January 2019	UL review update
Draft 0.3	April 2019	UL review update
Draft 0.4	April 2019	Update Section 7
V1.0	May 2019	Release version
V1.1	Nov 2019	Update Section 3
V1.2	May 2020	Removed unnecessary sections and Appendices
V2.0	March 2021	Designated Change to PCI SSC listed ADVAM P2PE Solution: - New devices Move/5000 V5.x, iUR250 V4.x, Open 1500 V5.x, Self/2000 V5.x, Self/4000 V5.x and Self/5000 V5.x - Update P2PE Application version from 1.0.* to 1.1.* ()
V2.1	May 2021	Page 1 Copyright updated Page 11 Reference for contact changed to ADVAM Support
V3.1	Nov 2021	- Updated the document with latest PIM 3.X template 2.2 Added New images - ADVAM package seals 3.2 – Application and Vendor version.
V3.2	April 2022	- Updated 3.2 POI Software/Application Details to include ADVAM Secure Card Processor 1.1.* - Added new ADVAM/TNS trusted locations.
V3.3	August 2022	- Updated 'ADVAM' branding to TNS - Updated TNS P2PE Application Version

Contents

Overview.....	5
Purpose and Intended Audience.....	5
PIM Review and Update Frequency	5
PIM Distribution to Merchants/Partners.....	5
How to Use this PIM.....	5
1 <i>P2PE Solution Information and Solution Provider Contact Details</i>	6
1.1 P2PE Solution Information	6
1.2 Solution Provider Contact Information	6
1.3 Solution Component Provider	6
2 <i>Confirm Devices were not tampered with and confirm the identity of any third-party personnel</i>	7
2.1 Instructions for ensuring POI devices originate from trusted sites/locations only.....	7
2.2 Instructions for confirming POI device and packaging were not tampered with, and for establishing secure, confirmed communications with the solution provider.	8
2.3 Instructions to confirm the business need for, and identities of, any third-party personnel claiming to be support or repair personnel, prior to granting those personnel access to POI devices.	10
3 <i>Approved POI Devices, Applications/Software, and the Merchant Inventory</i>	11
3.1 POI Device Details.....	11
3.2 POI Software/Application Details	12
3.3 POI Inventory & Monitoring	13
4 <i>POI Device Installation Instructions</i>	15
4.1 Installation and connection instructions	16
4.2 Guidance for selecting appropriate locations for deployed devices.....	18
4.3 Guidance for physically securing deployed devices to prevent unauthorized removal or substitution	18
5 <i>POI Device Transit</i>.....	19
5.1 Instructions for securing POI devices intended for, and during, transit.....	19
5.2 Instructions for ensuring POI devices are shipped to, trusted sites/locations only.....	21
6 <i>POI Device Tamper & Modification Guidance</i>.....	22
6.1 Instructions for physically inspecting POI devices and preventing skimming, including instructions and contact details for reporting any suspicious activity.....	22
6.2 Instructions for responding to evidence of POI device tampering	23
7 <i>Device Encryption Issues</i>.....	23
8 <i>POI Device Troubleshooting</i>	25
8.1 Instructions for troubleshooting a POI device	25

9 Additional Guidance..... 26

9.1 Instructions for troubleshooting a POI device 26

9.2 Instructions for how to confirm hardware, firmware, and application versions on POI devices 26

10 Glossary of Terms..... 27

11 Appendix A- ADVAM Support 29

ADVAM Support Contact Details 29

12 Appendix B - INSPECTION SHEET..... 30



Overview

Purpose and Intended Audience

This document is an instruction manual prepared by ADVAM in accordance with the PCI P2PE Standard to instruct customers (merchants), resellers/integrators and installers on secure ADVAM P2PE Solution implementation.

The manual aims to provision for secure configuration specifics, and to clearly delineate vendor, reseller/integrator and merchant responsibilities for installing and/or using the ADVAM P2PE Solution.

Merchants using the ADVAM P2PE Solution will minimise their PCI DSS compliance responsibilities but in doing so are required to adhere to this P2PE Instruction Manual (PIM), provided by ADVAM and/or an authorised integrator/reseller/installer partner.

NOTE: Although this manual relates predominantly to the merchant, it should be noted that instructions are also applicable to all entities that perform a function for and on behalf of the merchant. Integrator/resellers and installers must implement the ADVAM P2PE solution in compliance with both this PIM document and applicable requirements in the P2PE Program Guide.

PIM Review and Update Frequency

ADVAM **shall** review this document annually and additionally will review upon there being any changes to the ADVAM P2PE solution and or when notified of changes to the PCI P2PE Standard requirements documented herein.

ADVAM P2PE solution changes might include for example:

- additions or removals of P2PE POI device types,
- additions or removals of P2PE applications, and/or P2PE non-payment software,
- additions or removals of P2PE components.

PIM Distribution to Merchants/Partners

The ADVAM P2PE Instruction Manual will be provided to all merchants as part of the onboarding process.

Updates will be communicated to all affected merchants and ADVAM will provide merchants with an updated PIM as required or upon request.

How to Use this PIM

- Navigation and points of interest within this document:
- The word “**shall**”, is utilised throughout to represent an action that must be undertaken by the intended user in order to maintain compliance.
- **Note:** Notes are provided throughout the document to highlight an important point to the reader;
- Cross references are displayed as bolded [underlined text](#) which can be accessed by performing **CTRL+ Click** on the link.
- Appendices provide supplementary information and further guidance to the user.

1 P2PE Solution Information and Solution Provider Contact Details

1.1 P2PE Solution Information

Solution name:	<i>ADVAM P2PE Solution</i>
Solution reference number per PCI SSC website:	<i>2022-01248.006</i>

1.2 Solution Provider Contact Information

Company name:	<i>ADVAM Pty Ltd</i>
Company address:	<i>Level 2, 26 Franklin Street, Adelaide South Australia 5000</i>
Company URL:	<i>https://www.advam.com</i>
Contact name:	<i>Dan Billsdon</i>
Contact phone number:	<i>+61 434 308 149</i>
Contact e-mail address:	<i>dbillsdon@tnsi.com</i>

P2PE and PCI DSS

Merchants using this P2PE solution may be required to validate PCI DSS compliance and should be aware of their applicable PCI DSS requirements. Merchants should contact their acquirer or payment brands to determine their PCI DSS validation requirements.

1.3 Solution Component Provider

The Ingenico UK KIF (Ref# 2017-00470.019) & Ingenico US KIF(Ref# 2016-00470.017) are certified P2PE components that will be used as part of the ADVAM P2PE Solution. Refer to [P2PE Component Provider](#).

2 Confirm Devices were not tampered with and confirm the identity of any third-party personnel

2.1 Instructions for ensuring POI devices originate from trusted sites/locations only.

ADVAM, in partnership with Ingenico and its partners take all necessary precautions to ensure devices are not tampered with or compromised prior to being shipped.

Steps that must be undertaken to detect whether devices have been tampered with during transit.

1. Confirm that shipment of devices, have originated only from the trusted source and an authorised shipping partner – refer to alert received prior to receiving devices from courier:
 - Partner receives from ADVAM direct
 - Merchant receives from Partner direct

Trusted Location	ADDRESS
Ingenico US	Ingenico Group ,3025 Windward Plaza, Suite 600, Alpharetta, Georgia 30005, USA <u>UPS & FEDEX for delivery</u>
TNS US	10740 Parkridge Boulevard Suite 100 Reston, Virginia 20191, US
ADVAM UK	Fairbairn Building, 70-72 Sackville Street, Manchester, M1 3NJ United Kingdom
ADVAM AU	26 Franklin Street, Adelaide 5000 South Australia, Australia <u>TNT/FEDEX for delivery</u>

2. Match the source location address, the serial numbers on the terminal and the boxes/tamper packaging serial numbers the terminals are in to the shipment invoice notice received separately – Additionally, crosscheck all courier and reference details to the packing slip within the box
3. If the POI device originates from another source other than prior notification indicates, contact relevant sender (as per step 1)
4. If the shipping location cannot be confirmed as being authorised, then **DO NOT** deploy the device
5. Only authorised personnel should sign and receive the device from an authorised sender

2.2 Instructions for confirming POI device and packaging were not tampered with, and for establishing secure, confirmed communications with the solution provider.

Tamper Detection and Prevention Guidelines

Merchant and authorised Partners **shall** implement procedures, based on the guidelines provided within this manual, for the purpose of detecting unauthorised alterations (compromise) or replacement (substitution) of a device either pre, or post deployment.

It is recommended that the entity in custody of the device **shall** validate that the device received, stored or deployed has not been tampered with or substituted.

At all phases of the device lifecycle, secure tamper evident serialised packaging or suitable other secure means of security **shall** be in use.

At all times during device transit, the device receipting process must be preceded by tracking and device serial details being sent to the receiving entity by the sending entity, whether the sender is external or internal to the receiving entity.

Preventative measures throughout the device lifecycle can be summarised by the following section

Pre-deployment preventative measures:

- Confirm shipment origination to pre-shipped communication from sender records - [Confirm Where POI Device Originates From?](#)
- Validate upon receipt, the serial number of packaging to the details in the pre-shipped communication from the sender records
- Validate upon receipt that the tamper evident packaging is intact and is the same serialised number that was separately communicated by the sender prior to receipt
- Perform physical inspection of the device packaging to search for breakage of seals and security tampering seals
- Maintain device in original, tamper-evident packaging or physically store it in a secure location until ready for deployment
- Restrict access to authorised personnel only
- Maintain a log of all access to device, including personnel name, company, reason for access, time in and out.
- Record device in inventory-tracking system as soon as possible.
- Implement an audit trail, to demonstrate that a device is controlled, and not left unprotected, from receipt through to installation
- Prior to deployment into production, functionality must be tested to ensure that the device communicates and captures data properly
- Perform pre-installation inspection procedures, including physical and functional tests and visual inspection, to verify integrity of device with the

Post-deployment preventative measures:

Periodic inspection is performed **(90 days for unattended)** at deployed locations.

Compare the serial number of the device with the serial number recorded for the location

The connections to the device should be inspected to ensure no component other than those permitted under the ADVAM P2PE solution are attached

Check for missing or altered tamper seals or screws, extraneous wiring, holes in the device, or the addition of labels or other covering materials that could be used to mask damage from device tampering

Check for unauthorised device component connections

Check reader device for any skimmer device inserted.

Check PIN Pad for any overlay

Monitor devices in remote or unattended locations (for example, via the use of video surveillance or other physical mechanisms to alert personnel) –

If anything, suspicious is detected, the device **shall** be disconnected, immediately.

Report tampered or missing POI devices and other suspicious activity immediately to local law enforcement and the device provider - [Suspected substitution or missing device](#)

What to do if a device is received from an untrusted or unknown source location?

1. Notify ADVAM Support immediately
2. Follow RMA process

Images of tampered packaging

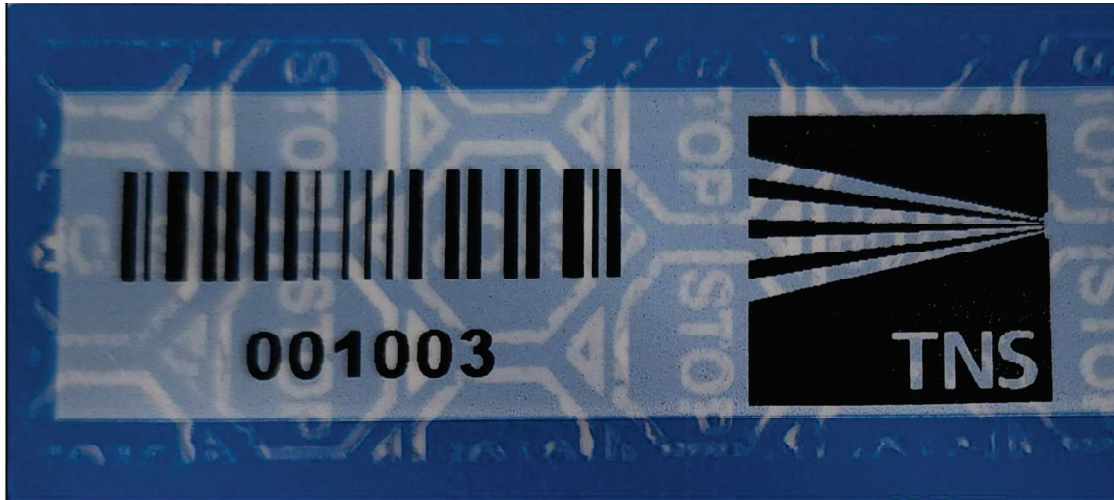


Image of Untampered for Comparison



In the Images above (see ADVAM stickers for comparison)

- 001003 is a Voided/Tampered seal.
- 001001 is a valid/unbroken seal.

NOTE: If you believe the packaging or the device has been tampered with, DO NOT deploy the device.

Physically secure POI devices in your possession for all devices including those :

- Awaiting deployment
- Undergoing repair or otherwise not in use
- Waiting transport between sites/locations

2.3 Instructions to confirm the business need for, and identities of, any third-party personnel claiming to be support or repair personnel, prior to granting those personnel access to POI devices.

To ensure there is no unauthorised third-party access to a device in production or a device about to be deployed to production, access **shall** be monitored. This is required to reduce the risk of device tampering, substitution or theft.

Third-Party Access Policy should encompass the following:

Each site manager shall be instructed, by their authorised merchant head office personnel, of the field service partner company and representative details, authorised to access, deploy or remove a POI device in production.

Merchant's head office personnel shall be responsible for informing, in advance, to the site manager, of any planned date for a scheduled maintenance operation at the deployment site level.

The authorised personnel of the field service company must provide proof of their identity prior to being allowed to handle any POI devices at the site being visited.

Authorised third-party personnel **shall** be escorted and monitored at all time whilst on site

Visits should be logged detailing:

- time in/out
- name of service provider and company
- proof of id used
- reason for the visit

Authorisation must be obtained prior to removal and or replacement of a device

Authorised replacement **shall** require physical inspection and inventory update processes to be performed.

*****IMPORTANT*****

If NO validation of identification of third-party can be completed then access must be denied to device/s

3 Approved POI Devices, Applications/Software, and the Merchant Inventory

3.1 POI Device Details

The following information lists the details of the PCI-approved POI devices approved for use in this P2PE solution.

All POI device information can be verified by visiting:

https://www.pcisecuritystandards.org/approved_companies_providers/approved_pin_transaction_security.php

See also Section 9.2, “Instructions for how to confirm hardware, firmware, and application versions on POI devices.”

PCI PTS approval #:	POI device vendor:	POI device model name and number:	Hardware version #(s):	Firmware version #(s):
4-30161	Ingenico	iUC285	IUC28x-01Txxxxx	820177V01.xx
4-30100	Ingenico	iUC180B	IUC1xx-11Txxxxx	SRED (CTLS):820305 V01.xx
4-30155	Ingenico	iUR255	iUR2xx-01Txxxxx, iUR2xx-11Txxxxx	820168 v01.xx
4-30075	Ingenico	iUP250	IUP2xx-01Txxxxx	820305 V01.xx, SRED: 820528V02.xx,
4-30251	Ingenico	iUP250LE	IUP2xx-11Txxxxx	820305v12.xx, 820305V13.xx
4-30083	Ingenico	iUR250	iUR2xx-01Txxxxx	SRED: 820514V01.xx, 820514V11.xx
4-30250	Ingenico	iUR250	iUR2xx-01Txxxxx	SRED: 820514V02.xx, 820514V12.xx, 820365V02.xx
4-30172	Ingenico	iUC150B	iUC15x-01Txxxxx	820168 v01.xx
4-30157	Ingenico	iUI120	iUI1xx-01Txxxxx	820167 v11.xx
4-30160	Ingenico	iUC280	IUC28x-01Txxxxx	820176 v01.xx, SRED: 820365 V02.xx
4-20316	Ingenico	Move/5000	MOV50JB (CTLS + Privacy shield + Desktop case lid)	820376v01.xx, 820547v01.xx, 820549v01.xx (SRED OnGuard FPE), 820555v01.xx (SRED), 820556v01.xx (SRED OnGuard SDE), 820559v01.xx (SRED ANL), 820565v01.xx (SRED FF1), 820548V02.xx (Open Protocol), 820548v03.xx, 820548V06.xx
4-30349	Ingenico	Open 1500	OPE15BA (OPEN1500)	820547v01.xx, 820376v01.xx (Schemes), 820548V03.xx (OP), 820556v01.xx (SRED On- Guard SDE), 820549v01.xx (SRED On- Guard FPE)
4-30381	Ingenico	Self/2000	SEL20AA	820566v01.xx

4-30393	Ingenico	Self/4000	SEL40BA	820547v01.xx
4-30384	Ingenico	Self/5000	SEL50CA	820566v01.xx

3.2 POI Software/Application Details

The following information lists the details of all software/applications (both P2PE applications and P2PE non-payment software) on POI devices used in this P2PE solution.

All applications with access to clear-text account data must be reviewed according to Domain 2 and are included in the P2PE solution listing. These applications may also be optionally included in the PCI P2PE list of Validated P2PE Applications list at vendor or solution provider discretion.

Application Vendor, Name, and Version #	POI Device Vendor	POI Device Model Name(s) and Number:	POI Device Hardware & Firmware Version #	Is Application PCI Listed? (Y/N)	Does Application Have Access to Clear-text Account Data (Y/N)
ADVAM Secure Card Processor 1.3.*	Ingenico	iUC180B PCI PTS V3.x iUP250 PCI PTS V3.x iUP250LE PCI PTS V4.x iUI120 PCI PTS V4.x iUC285 PCI PTS V4.x Move/5000 V5.x Open/1500 V5.x Self/2000 V5.x Self/4000 V5.x Self/5000 V5.x	Refer to section 2 above for hardware details against each device	Y	
ADVAM Secure Card Processor 1.2.*	Ingenico	iUC180B PCI PTS V3.x iUP250 PCI PTS V3.x iUP250LE PCI PTS V4.x iUI120 PCI PTS V4.x iUC285 PCI PTS V4.x Move/5000 V5.x	Refer to section 2 above for hardware details against each device	Y	

3.2 POI Software/Application Details

		Open/1500 V5.x Self/2000 V5.x Self/4000 V5.x Self/5000 V5.x			
ADVAM Secure Card Processor 1.1.*	Ingenico	iUC180B PCI PTS V3.x iUI120 PCI PTS V4.x iUP250LE PCI PTS V4.x iUC285 PCI PTS V4.x Move/5000 V5.x Open/1500 V5.x Self/2000 V5.x Self/4000 V5.x Self/5000 V5.x	Refer to section 2 above for hardware details against each device	Y	

3.3 POI Inventory & Monitoring

All POI devices must be documented via inventory control and monitoring procedures, including device status (deployed, awaiting deployment, undergoing repair or otherwise not in use, or in transit).

This inventory must be performed annually, at a minimum.

Any variances in inventory, including missing or substituted POI devices, must be reported to [ADVAM Pty Ltd](#) via the contact information provided under [ADVAM Support Contact Details](#).

Sample inventory table below is for illustrative purposes only. The actual inventory should be captured and maintained by the merchant in an external document.

Sample Inventory Table

Device Vendor	Device Model Name(s) and Number	Device Location	Device Status	Serial Number or Other Unique Identifier	Date of Inventory
Ingenico	iUC150B	Stock storage (H/O)	Pre-deployment	16151UN20195167	11/10/2018
Ingenico	iUC150B	The Plaza (Park A)	Deployed	16151UN20195231	11/10/2018
Ingenico	iUC150B	The Plaza (Park B)	Deployed	16151UN20195153	11/10/2018
Ingenico	iUC150B	The Plaza (Staff)	In Transit - Deployment	16151UN20195222	11/10/2018
Ingenico	iUC150B	Ingenico Repair	Repair	16151UN20195250	11/10/2018
Ingenico	iUC150B	ADVAM Repair	Repair	16151UN20195255	11/10/2018

Physical Inventory Stock Take

Physical device stock counts are to be performed annually as a minimum to confirm that inventory reporting of devices is being recorded correctly.

The inventory stock count will:

confirm device transition in and out of service and or from one location/site to another;

confirm that all devices identified as being within your environment are currently within your possession and not missing;

- assist in detecting unauthorised removal, tampering or substitution of devices.

Device Inventory Variation

Any variances in inventory, including any identified missing or substituted device, or a detected compromised device, shall:

be reported to ADVAM Support Contact Details immediately; and

follow the instructions under the section Suspected substitution or missing device

4 POI Device Installation Instructions

Do not connect non-approved cardholder data capture devices.

The P2PE solution is approved to include specific PCI-approved POI devices. Only these devices denoted above in Table 3.1 are allowed for cardholder data capture.

If a merchant's PCI-approved POI device is connected to a data capture mechanism that is not PCI approved, (for example, if a PCI-approved SCR was connected to a keypad that was not PCI-approved):

The use of such mechanisms to collect PCI payment-card data could mean that more PCI DSS requirements are now applicable for the merchant.

Only P2PE approved capture mechanisms as designated on PCI's list of Validated P2PE Solutions and represented in this PIM document can be used.

Do not change or attempt to change device configurations or settings.

Changing device configurations or settings may invalidate the PCI-approved P2PE solution in its entirety. Examples include, but are not limited to:

Enabling any device interfaces or data-capture mechanisms that were disabled on the P2PE solution POI device.

Altering security configurations or authentication controls on the POI device.

Physically opening the POI device.

Attempting to install unauthorized applications onto the POI device.

ADVAM P2PE Solution Logical Access Restrictions for Merchants

Merchant logical access to POI devices is restricted as follows:

- Read-only
- View transaction-related data
- Cannot view or access cryptographic keys
- Cannot view or access clear-text PAN
- Cannot view or access SAD.
- Cannot view or access device configuration settings that could impact the security controls of the device, or allow access to cryptographic keys or clear-text PAN and/or SAD
- Cannot enable disabled device interfaces or disabled data-capture mechanisms

4.1 Installation and connection instructions

Installation Guidelines

It is imperative that you follow the guidelines provided for the deployment of the ADVAM P2PE solution.

Failure to do so may impact your PCI DSS compliance and the protections afforded to you by the ADVAM P2PE solution.

The P2PE solution provided by ADVAM can only include those devices previously identified in section 2. It does not allow for POI components that are not PCI approved.

****IMPORTANT****

It must be understood that if a PCI-approved POI component is connected to another non-PCI approved device or data-capture mechanism, the non-PCI-approved capture mechanism is not secured by the ADVAM P2PE solution.

The use of any such mechanisms to collect PCI payment-card data would negate any PCI DSS scope reduction which might otherwise have been provided by the ADVAM P2PE solution's device.

Prior to deployment, you must understand that any modification to the deployment can and will impact

your compliance. Such modifications may include:

- Attempting to enable any device interfaces or data-capture mechanisms that were disabled on the P2PE solution POI device
- Attempting to alter security configurations or authentication controls
- Physically opening the device
- Attempting to install applications onto the device

Pre-Installation

1. Maintain device in original or new, tamper-evident packaging and physically store it in a secure location until ready for deployment and restrict access to authorised personnel
2. Check that all items in the box match the packing slip when unpacking the device.
3. Validate that serial numbers of received devices match sender records
4. Logging and tracking requirements:
 - Record device in inventory-tracking system as soon as possible.
 - Maintain a log of all access to device, including personnel name, company, reason for access, time in and out.
5. Implement an audit trail, to demonstrate that a device is controlled, and not left unprotected, from receipt through to installation.
6. Refer to Ingenico installation user guide and product guide to ensure secure installation
7. It is important to ensure that the operating environment conditions follow those specified in the Ingenico installation user guide provided with the terminal.
8. Prior to connecting the terminal, checks should be made to verify the overall status and integrity of the device.

Checks should include but not be limited to ensuring that:

- The keypad is firmly in place and there is no visual evidence of tampering;
- Perform physical and functional tests and visual inspection,
- There is no evidence of unusual wires connected to any ports on the terminal or associated equipment, the chip card reader or any other part of the terminal.

NOTE: It is recommended that these checks are performed on a regular basis post installation.

If the device serial number is not visible once integrated into the merchant environment, merchant managed serialised labels should be used to enable quick identification of POI devices for inventory or inspection purposes, avoiding having to disconnect the terminal.

Install the POI device and verify at power-up that no intrusion message appears on the screen. If you see a message such as one displayed on the screen below, immediately disconnect the device and contact ADVAM support.

The POI device contains tamper mechanisms that will be triggered when a physical penetration attempt of the device is detected. The activation of tamper mechanisms will make the device become “non-activated mode”.

If the device is placed into a “non-activated mode” it can be presumed that:

the device is tampered,

not operating and

needs reactivation after maintenance and security checks.

The POI device will detect any “tampered state” and if the device is tampered, the terminal, will repeatedly flash the message, “Alert Interruption!!!” and any further use of the terminal will not be possible.



Alert on Telium2 device

Note: Only PCI-approved POI devices listed in the PIM are allowed for use in the P2PE solution for account data capture.

4.2 Guidance for selecting appropriate locations for deployed devices

The location where the terminal is deployed must be sufficiently secure, to deter theft or compromise of the device.

The following **recommendations** for secure deployment are provided:

Control public access to the devices such that access is limited to only parts of the device a person is expected to use to complete a transaction (for example, PIN pad and card reader).

Locate the devices so they can be observed/monitored by authorised personnel.

Bolt down devices which are stationary (unattended)

Locate devices in an environment that deters compromise attempts—for example, through lighting, access paths and other visible security measures such as 24/7 CCTV surveillance.

Note: As per PCI issued “Information Supplement: Skimming Prevention: Best Practices for Merchants version 2.0” it is **strongly recommended** that remote or unattended devices be in view of a surveillance camera, to deter anyone from tampering with the device, however, steps should be taken to ensure surveillance/CCTV cameras and staff cannot see the screen or the PIN entry pad on the device.

4.3 Guidance for physically securing deployed devices to prevent unauthorized removal or substitution

Once a merchant or authorised partner takes possession of a device, it is thereafter, their responsibility to manage the physical security of that device. The exception to this is where the device is shipped back to Ingenico/ADVAM or to an ADVAM authorised Partner, or when arrangements have been made between ADVAM and the merchant for the ongoing management of the devices on the merchant’s behalf.

If the device is deployed in a remote location or unattended, it is recommended that it is monitored with a camera so that footage can be reviewed to determine if someone has attempted to tamper with the device.

When not in use, the device **shall** be placed in a secure location that can be locked and made completely inaccessible other than to authorised personnel.

Examples of processes and controls required to prevent and deter unauthorised removal or substitution of devices:

- Perform regular inspections of the device and cable connections
- Maintain a log of inspections which are dated and signed by authorised personnel
- Check that the device serial number is correct and that the labels have not been tampered with
- Asset register control and regular stocktake controls
- Device Tracking controls
- It is strongly recommended to monitor the device location with continuous CCTV and alert capability - provide for detection of lost or stolen equipment and notification to authorised personnel

Note: As per PCI issued “Information Supplement: Skimming Prevention: Best Practices for Merchants version 2.0” it is **strongly recommended** that remote or unattended devices be in view of a surveillance camera, to deter anyone from tampering with the device, however, steps should be taken to ensure surveillance/CCTV cameras and staff cannot see the screen or the PIN entry pad on the device. Please also note that having security camera and personnel monitoring the area does not

remove the applicability of PCI DSS Requirement 9.9.2 (Periodically inspect devices surfaces to detect tampering, or substitution).

Suspected substitution or missing device

ADVAM Authorised Partner (Reseller/Integrator) and Merchant Response

If a POI device is missing or is suspected of being substituted, immediately follow these steps:

Contact [ADVAM Support](#) Contact Details to report the incident

Installer is to raise a Support ticket to ADVAM Support – advam-support@tnsi.com

Provide following details

- .1 POI device serial number
- .2 device site location
- .3 Equipment reference number

Follow RMA process – and send to ADVAM

Merchant is to register the device as Status = “Missing” in the inventory report

5 POI Device Transit

5.1 Instructions for securing POI devices intended for, and during, transit

When shipping devices between locations/sites for deployment or for return, devices must be shipped securely.

Devices **shall** be packed in tamper-evident serialised packaging or similar, for tracking purposes and shipped in a secure manner by using a secure transit method.

1. Merchant/Authorised Partner **shall** Pack devices in tamper-evident serialised packaging prior to transit or source suitable other secure means of security for transit



example of tamper evident serialised packaging

2. Merchant/Authorised Partner **shall** secure POI devices in transit (return to vendor, manufacturer or transfer between locations), by using one of the following transit methods:
 - a. Shipping via a trackable shipping option using either:
 - a private courier service or
 - public shipping company that provides the status of the package during shipping.
 - b. Transferring between sites using an **authorised** employee known by the receiving employee.

Note: If using internal employees as a device shipment method, instruct staff to not leave devices in public areas unattended, for example, in view on a car seat or at company reception areas. This may lead to unauthorised access or theft of the device.

3. Log the following tracking information:
 - Personnel providing shipping (name and title)
 - Serial number of tamper bag
 - Date of Pickup
 - Courier Company
 - Make, model and serial number of the device being shipped
 - Confirmation Date of Delivery

- Sender is to communicate (email), in advance, to the receiving entity, the shipping details such as the courier package tracking reference number and the tamper evident bag serial number.
- Receiving entity is to confirm receipt (email) of devices to the sender
- The receiving entity **shall** validate upon receipt that the tamper evident seals, packaging etc. is intact and is the same information that was separately communicated by the sender prior to shipping.
Note: Devices received without prior shipping confirmation being received or where devices are delivered in a manner unexpected, the receiver **shall** confirm with the sender prior to deployment of the devices.
- Procedures **shall** be in place for determining whether device packaging has been tampered with. Personnel are to be trained on how to investigate for breakage of tamper-evident seals on the external packaging and to investigate the device itself for cracks or breakage of security seals.

Physically secure POI devices in your possession, including devices:

- Awaiting deployment
- Undergoing repair or otherwise not in use
- Waiting transport between sites/locations

5.2 Instructions for ensuring POI devices are shipped to, trusted sites/locations only

Confirm Where POI Device Originates From?

ADVAM, in partnership with Ingenico and its partners take all necessary precautions to ensure devices are not tampered with or compromised prior to being shipped.

Steps that must be undertaken to detect whether devices have been tampered with during transit.

1. Confirm that shipment of devices, have originated only from the trusted source and an authorised shipping partner – refer to alert received prior to receiving devices from courier:
 - Partner receives from ADVAM direct
 - Merchant receives from Partner direct

Trusted Location	ADDRESS
Ingenico US	Ingenico Group ,3025 Windward Plaza, Suite 600, Alpharetta, Georgia 30005, USA <u>UPS & FEDEX for delivery</u>
TNS US	10740 Parkridge Blvd STE 100, Reston, VA 20191, United States
ADVAM UK	Transaction Network Services 5 Europa View, Sheffield. S9 1XH, UK
ADVAM AU	26 Franklin Street, Adelaide 5000 South Australia, Australia <u>TNT/FEDEX for delivery</u>

2. Match the source location address, the serial numbers on the terminal and the boxes/tamper packaging serial numbers the terminals are in to the shipment invoice notice received separately – Additionally, crosscheck all courier and reference details to the packing slip within the box
3. If the POI device originates from another source other than prior notification indicates, contact relevant sender (as per step 1)
4. If the shipping location cannot be confirmed as being authorised, then **DO NOT** deploy the device
5. Only authorised personnel should sign and receive the device from an authorised sender

6 POI Device Tamper & Modification Guidance

6.1 Instructions for physically inspecting POI devices and preventing skimming, including instructions and contact details for reporting any suspicious activity

Additional guidance for inspecting POI devices can be found in the document entitled *Skimming Prevention: Best Practices for Merchants*, available at www.pcisecuritystandards.org.

Skimmers are devices used by attackers to capture cardholder data prior to the POI device reading the card. Skimmers may be inserted in the MSR of the device or overlaid on the device itself. For further guidance

NOTE: Merchants **shall** train personnel interfacing with the POI devices, on a regular basis, to inspect deployed POI devices for any evidence of tampering or skimmer devices.

- Merchants **shall** perform regular physical inspections on POI devices to detect any tampering, compromise or modification.

NOTE: It is recommended that the frequency of inspections be 90 days for unattended.

- During the inspection, the integrity of the device must be checked, including the compartments, provided that the compartments can be accessed after the devices are deployed.
- Inspection sheets of terminals listed in section 2 are attached, for an indication of the correct position and size of seals, labels, and screws that **shall** be verified. **Refer to Appendix B - INSPECTION SHEET for reference images**
- If the POI device is attached to a stand or equipment and cannot be removed without removing the screws, it does not need to be detached for physical inspection. The inspection can be restricted to the visible, however, the POI device **shall** be tracked with a single identifier (lock serial number, label serial number, etc.) which is clearly visible to the merchant i.e. merchant managed serialised labels
- Never allow unauthorised persons to access the device under any circumstance. Merchants **shall** always confirm the identity of a service engineer by contacting their authorised Partner.
- If possible, it is recommended that devices, upon receipt, will be weighed and checked against the default weights (if not already mounted into equipment).

Physical Device Inspection

1. Physical inspection consists of a visual inspection of the device's casing and connections:
 - check general device status (sign of breach, alteration, holes, etc.)
 - check for missing or altered seals or screws
 - check the integrity of the visible seals (if any)
 - verify that no wiring, antenna, or extraneous modules have been added to the device
 - verify that no unauthorised devices are attached to the POI device
 - check for the addition of labels
 - check other covering material that could be used to mask damage from device tampering,
 - check that the serial number label, when accessible, does not show any alteration.
 - check merchant managed serialised labels for tampering
 - compare device information with the inventory information recorded (ongoing inspections)
2. Remote or unattended devices should be monitored via continuous video surveillance and or other mechanisms which will provide an alert mechanism to merchant personnel.

Reporting Suspicious Activity - Who to Contact?

Suspicious activity, can include but not be limited to:

- Physical device breach
- Logical alterations to device (configuration, access controls)
- Disconnection or reconnection of devices
- Failure of encryption mechanism
- Failure of any device security control
- Connection of unrecognized device

Contact details and instructions for reporting suspicious activity and returning the device:

- Immediately contact the ADVAM Support directly
- Contact details and instructions for returning devices to ADVAM

Description to be **“Special RMA- Tamper Evidence for investigation and repair”**

6.2 Instructions for responding to evidence of POI device tampering

Device Tamper Response

If, during the physical inspection of a device (pre and post deployment), any suspicion or sign of tampering is detected then the following response is required:

1. The deployed device shall be immediately disconnected from all networks or the new device shall not be deployed
2. Contact ADVAM Support, refer to link - [Appendix A- ADVAM Support](#)
3. Provide all serial and device location details
4. A ticket shall be raised to ADVAM Support with the serial number of the device, and a photograph of the breach or suspected breach provided.
5. ADVAM Support will then provide instructions to return the compromised device to ADVAM.
 - Securely package the device in a tamper-evident serialised bag
 - Return the device as per RMA instructions – refer to link

Device Permanently Removed from Service – Secure Destruction Transit

Devices **shall** be returned to ADVAM for destruction.

Disposal of devices will be handled by ADVAM and or authorised parties including Ingenico UK.

The Merchant/Partner **shall** take the following steps:

1. Contact ADVAM Support [Appendix A- ADVAM Support](#)
2. Follow the RMA request process – refer to link
3. Return the device to Ingenico with the description being “Special RMA- Secure Destruction”.
4. Prepare the device for shipping - tamper-evident secure packaging.
5. Use a trackable courier for return of device for the trusted shipping partners mentioned in Section 4

7 Device Encryption Issues

7.1 Instructions for responding to POI device encryption failures

NOTE: ADVAM does not support a method for disabling P2PE encryption for the environment. The preference is to transition to a non-P2PE environment outside of this solution which is PCI DSS compliant.

1. Once the POI device is provisioned as a P2PE terminal within the ADVAM solution and an encryption failure is experienced,
 - the transaction/s will be aborted.
 - the error **shall** be recorded by the merchant and reported to the ADVAM Support team, who will troubleshoot the incumbent transaction/s.
2. If there is a provisioning issue encountered and the terminal is not declared a P2PE terminal, resulting in transactions (cardholder data) not being encrypted, ADVAM's monitoring system will raise an alert to the ADVAM support team.
3. Once ADVAM detects an issue with encryption at the POI device and or decryption at the HSM, ADVAM's preference is to implement Option 1 below.

Option 1:

- troubleshooting to remedy the issue;
- inform the impacted merchant that the POI device cannot be used to capture credit card data;
- take the impacted POI device offline so that it can no longer accept credit card data while ADVAM is fixing the issue.

NOTE: If this approach is accepted by the merchant, then the merchant will still be considered to be using a P2PE solution and their PCI DSS compliance will not be impacted.

Option 2:

The merchant can exercise the right to continue to use the ADVAM POI device to capture credit card payments where encryption on the device is requested to be disabled.

In this situation the merchant would be deemed to **not** be using a P2PE solution and their PCI DSS compliance would be impacted until P2PE functionality is restored by ADVAM. The impact might be that the merchant would be subject to all applicable PCI DSS requirements while they are not using an approved P2PE solution.

NOTE: ADVAM will only disable encryption once the Merchant provides a written request to opt out as per PCI P2PE requirement 3A-4

Once the POI device is P2PE activated on the ADVAM P2PE solution, merchants do not have the option to disable the P2PE capability on their own.

Merchants may stop P2PE encryption of account data only by providing a written request, signed by a merchant executive officer, to the ADVAM Support team which instructs ADVAM to disable P2PE encryption functionality on its complete estate (as per PCI P2PE Standard requirement 3A-4.x).

The notification letter shall state that the merchant accepts responsibility for the following:

1. The security impact to the merchant's account data and potential risks associated with processing transactions without P2PE protection.
2. Responsibility for implementing alternative controls and or processing methods, in order to protect account data in lieu of the P2PE solution.
3. That the merchant is no longer eligible for completing SAQ P2PE, associated with use of PCI P2PE solutions.
4. Advising their acquirer that they are no longer using the P2PE solution.
5. Understanding that processing transactions without P2PE protection may impact the merchant's PCI DSS compliance validation
6. Confirm with their acquirer or payment brand, as applicable, for all PCI payment brands affected.

To formally request that encryption of account data be stopped, the following information will be required:

- Merchant ID (or all Merchant IDs if more than one)
- Total number of devices
- Make and Model of devices
- Serial Numbers of all devices

NOTE: Once the opt out instruction letter is acknowledged by ADVAM, ADVAM shall disable the P2PE feature centrally and remotely upgrade all POI devices of the estate to disable encryption

8 POI Device Troubleshooting

8.1 Instructions for troubleshooting a POI device

In the event of an issue, ADVAM will work with you remotely to troubleshoot the issue. Prior to any troubleshooting, ADVAM will confirm that the individual contacting us is an authorised individual within your organisation for troubleshooting purposes as defined to us during the initial deployment of the solution.

During the troubleshooting process:

- PAN and/or SAD is never output to the merchant environment
- Collection of PAN and/or SAD only when needed to solve a specific problem.
- Data collected will be encrypted whilst stored
- Storage of such data only in specific, known locations with limited access.
- Collection will be of only a limited amount of data needed to solve a specific problem.
- Secure deletion of such data from storage immediately after use and issue resolved

NOTE: Logs to be collected will be collected automatically from the device, and these will not contain cardholder data.

The merchants shall not deliver clear-text cardholder data to ADVAM even if requested.

9 Additional Guidance

9.1 Instructions for troubleshooting a POI device

In the case where a POI device malfunctions unexplainably or some form of setup problems are experienced, the Partner **shall** raise a support ticket to ADVAM Support, using the contact information provided, refer to link [Appendix A- ADVAM Support](#)

9.2 Instructions for how to confirm hardware, firmware, and application versions on POI devices

[See Appendix B - INSPECTION SHEET](#)

Glossary of Terms

Term/Acronym	Description
Component Provider	A Third-Party Service Provider is only considered a P2PE Component Provider for eligible P2PE Component services if the applicable service is separately PCI-listed on the List of Validated P2PE Components.
Customer	Merchants are the P2PE Solution customers and users
Encryption	The (reversible) transformation of data by a cryptographic algorithm to produce cipher text— i.e., hiding the information content of the data.
Estate Manager	Management of Terminal software
Firmware	Firmware is considered to be any code within the POI device that provides security protections needed to comply with PTS device security requirements or can impact compliance to these security requirements.
Integrator/Reseller	Integrators and Resellers are those entities that sell, install, and/or service P2PE Solutions on behalf of P2PE Vendors or others. Integrators
KIF	Key Injection Facility. Entities that perform cryptographic key injection for POI Devices.
Third-Party service provider	An entity that provides a service or function on behalf of a P2PE Solution Provider, which is incorporated into and/or referenced by the applicable P2PE Solution, such as a payment gateway or data centre.
P2PE Components	P2PE service (such as encryption management, decryption management, or key injection) that is eligible for validation and acceptance on a standalone basis as part of the P2PE Program and which may be incorporated into and/or referenced as part of a P2PE Solution.
P2PE Solution	A combination of secure devices, applications, and processes that encrypt cardholder data from a PCI-approved point-of-interaction (POI) device through to decryption, assessed in accordance with PCI's P2PE standard and included on PCI's list of Validated P2PE Solutions.

Term/Acronym	Description
PCI P2PE	Point to Point Encryption standard
PIG	P2PE Application Instruction Guide is specific to the ADVAM P2PE payment application for (US/UK/AU) region. The PIG provides instructions on how to implement the application in a secure and compliant manner. The instructions provided will be accurate and effective enough to enable the intended audience to be able to install and configure the application securely.
PIM	P2PE Implementation Manual is an instruction manual prepared by ADVAM in accordance with the PCI P2PE Standard to instruct customers (merchants) and resellers/integrators on secure ADVAM P2PE Solution implementation.
POI Device	Point of Interaction Device. Device used to accept payment card data for payment purposes. The initial point where data is read from a card.
RMA	Returned Materials Authorisation is the request process to follow when a device is to be returned for maintenance
Sensitive Data	Cardholder data containing the full PAN and sensitive authentication data (SAD) elements that may be transmitted or processed as part of a payment transaction
SBOM	SBOM number is the unique P2PE SKU This part number includes things like software loads, data packages, key injection requirements, and communication settings.
Tamper Evident Tape	Tape with a characteristic that provides evidence that an attack has been attempted such as trying to open a package.

Appendix A- ADVAM Support

As an ADVAM customer, you benefit from ADVAM's proven commitment to providing merchants with superior service and product support.

Our support team recognises the importance of fast, effective responses in allowing you to provide the best experience for your own customers.

ADVAM Support Contact Details

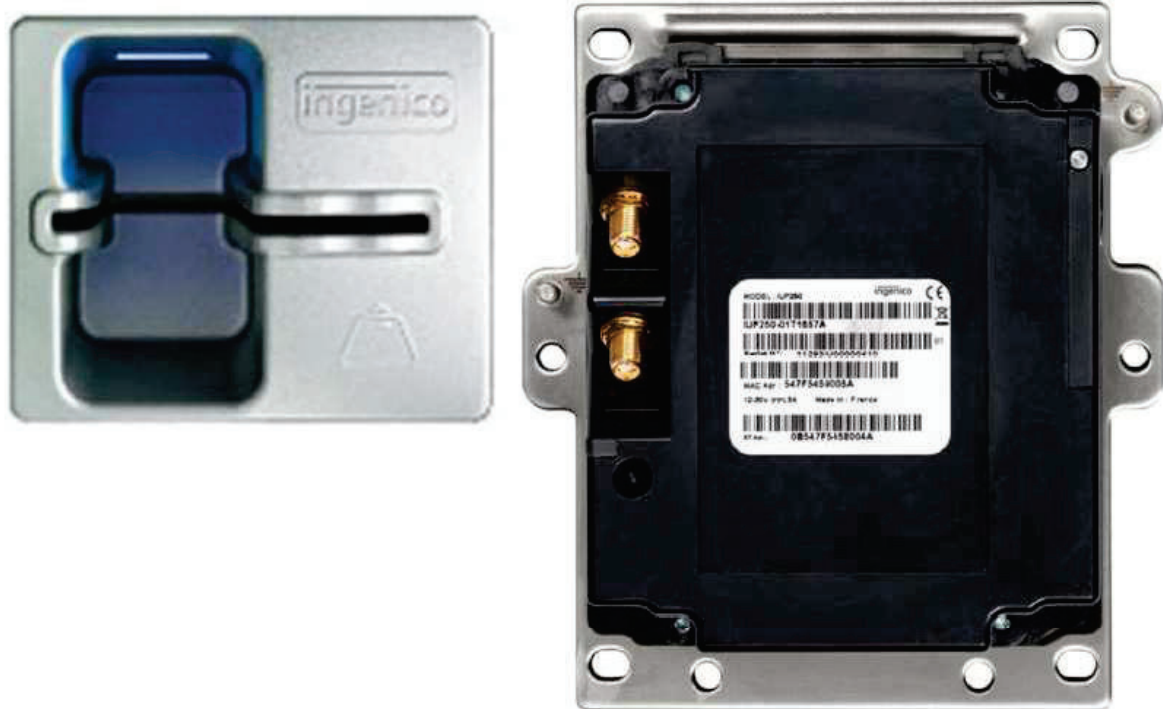
The details of our support team are as follows:

Contact Medium	Locations
Email	For UK: advam-support-uk@tnsi.com For US: advam-support-us@tnsi.com For AU: advam-support@tnsi.com
Telephone	+61-1300 130 778 (AU) +1-703 592 1251 (US) +44 330 016 0337 (UK)
Web	www.advam.com

NOTE: For email processing purposes, please ensure emails are titled as “**Attention: Unattended Payments**” – with a summarised **Subject/title**”

Appendix B - INSPECTION SHEET

12.1.1.1 iUR250 (iUP250)



Product hardware version ID is printed on a label at the back of the device. It must not be removed, altered or covered up.

12.1.1.2 iUP250LE



Product hardware version ID is printed on a label at the back of the device. It must not be removed, altered or covered up.

12.1.1.3 iUP250



Product hardware version ID is printed on a label at the back of the device. It must not be removed, altered or covered up.

12.1.1.4 iUC180B



Contactless LEDs are visible from the top



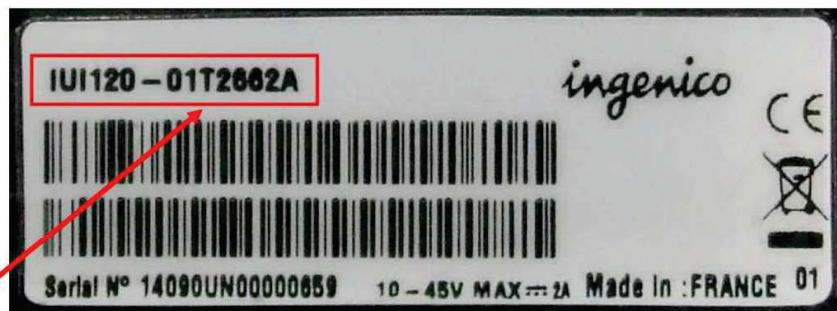
Product hardware version ID is printed on a label at the back of the device. It must not be removed, altered or covered up.

12.1.1.5 iUC150B



Product hardware version ID is printed on a label at the back of the device. It must not be removed, altered or covered up.

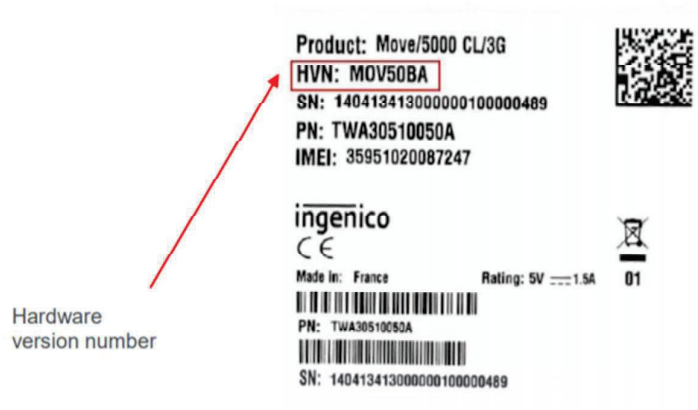
12.1.1.6 iUI120



Hardware version
Number

Product hardware version ID is printed on a label on the side of the device. It must not be removed, altered or covered up.

12.1.1.7 Move/5000

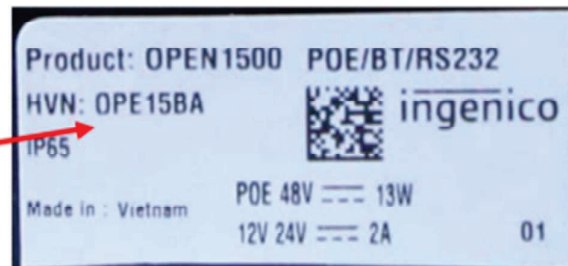


Product hardware version ID (HVN) is printed on a label at the back of the device. It must not be removed, altered or covered up.

12.1.1.8 Open/1500



Hardware version number



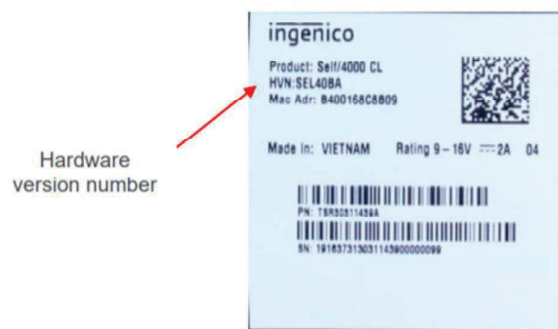
Product hardware version ID (HVN) is printed on a label at the back of the device. It must not be removed, altered or covered up.

12.1.1.9 Self/2000



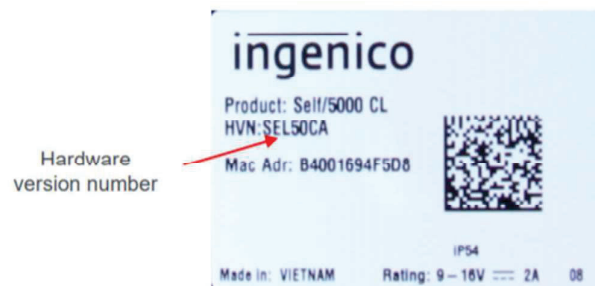
Product hardware version ID (HVN) is printed on a label at the back of the device. It must not be removed, altered or covered up.

12.1.1.10 Self/4000



Product hardware version ID (HVN) is printed on a label at the back of the device. It must not be removed, altered or covered up.

12.1.1.11 Self/5000



Product hardware version ID (HVN) is printed on a label at the back of the device. It must not be removed, altered or covered up.

- Waiting transport between sites/locations



EXHIBIT 6 TO SERVICE SCHEDULE
TNS' CERTIFICATE OF INSURANCE



CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)

05/28/2025

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER MARSH RISK & INSURANCE SERVICES FOUR EMBARCADERO CENTER, SUITE 1100 CALIFORNIA LICENSE NO. 0437153 SAN FRANCISCO, CA 94111 CN102555145-Koch-CasCy-24-25	CONTACT NAME: PHONE (A/C, No, Ext): FAX (A/C, No): E-MAIL ADDRESS: INSURER(S) AFFORDING COVERAGE INSURER A: Old Republic Insurance Company INSURER B: Swiss Re Corporate Solutions Capacity Insurance INSURER C: INSURER D: INSURER E: INSURER F:
INSURED Transaction Network Services, Inc. 4111 E. 37th Street North Wichita, KS 67220	NAIC # 24147 34916

COVERAGES**CERTIFICATE NUMBER:**

SEA-004101925-02

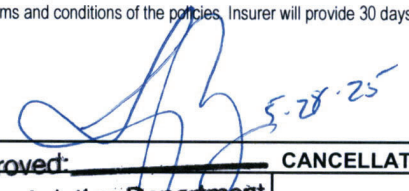
REVISION NUMBER: 2

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL SUBR INSD WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	☒ COMMERCIAL GENERAL LIABILITY ☐ CLAIMS-MADE ☒ OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: ☒ POLICY ☐ PRO-JECT ☐ LOC OTHER:	Y Y	MWZY 315812 24	12/01/2024	12/01/2025	EACH OCCURRENCE \$ 5,000,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$ 5,000,000 MED EXP (Any one person) \$ 10,000 PERSONAL & ADV INJURY \$ 5,000,000 GENERAL AGGREGATE \$ 5,000,000 PRODUCTS - COMP/OP AGG \$ 5,000,000
A	☒ AUTOMOBILE LIABILITY ☒ ANY AUTO ☐ OWNED AUTOS ONLY ☐ SCHEDULED AUTOS ☐ HIRED AUTOS ONLY ☐ NON-OWNED AUTOS ONLY	Y Y	MWTB 315811 24	12/01/2024	12/01/2025	COMBINED SINGLE LIMIT (Ea accident) \$ 5,000,000 BODILY INJURY (Per person) \$ BODILY INJURY (Per accident) \$ PROPERTY DAMAGE (Per accident) \$
	☐ UMBRELLA LIAB ☐ OCCUR ☐ EXCESS LIAB ☐ CLAIMS-MADE ☐ DED ☐ RETENTION \$	Y Y				EACH OCCURRENCE \$ AGGREGATE \$
A	☒ WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	Y/N N N/A	MWC 314306 24	12/01/2024	12/01/2025	☒ PER STATUTE ☐ OTH-ER E.L. EACH ACCIDENT \$ 1,000,000 E.L. DISEASE - EA EMPLOYEE \$ 1,000,000 E.L. DISEASE - POLICY LIMIT \$ 1,000,000
B	Tech E&O/Cyber		5376.11	12/01/2022	12/01/2025	Limit each claim/aggregate 5,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

Broward County and Fort Lauderdale-Hollywood International Airport, 320 Terminal Drive, Suite 200, Fort Lauderdale, FL 33315 are included as additional insureds on a primary and non-contributory basis with respect to the general liability, automobile liability and Tech E&O/Cyber policies but only as required by executed written contract and subject to the terms and conditions of the policies. A waiver of subrogation applies for all policies referenced above in accordance with the terms and conditions of the policies. Insurer will provide 30 days written notice of cancellation to certificate holder for any statutorily permitted reason other than nonpayment of premium.

CERTIFICATE HOLDERApproved: **CANCELLATION**

Broward County
320 Terminal Drive
Suite 200
Fort Lauderdale, FL 33315

Aviation Department
Tracy Meyer, Esq.
Risk Insurance and
Contracts Manager

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

Marsh Risk & Insurance Services

DISCLOSURE ITEMS FOR TNS SERVICE AGREEMENT

ISSUE	DISCLOSURE & APPLICABLE CONTRACT LANGUAGE
Term	Initial Term of 3 years, with two one-year renewal options by County. Agreement may not be reviewed if total compensation projected to be paid by County to TNS would exceed an aggregate total of \$500,000. County to track timing of renewal and expenditure. If County intends to extend further or reaches spending limit, then it would need to go to the BOCC for approval. (Section 1(a))
Termination	No termination for convenience. Instead, County may terminate Agreement on 90 days' notice at any time after the Initial Term of 36 months. (Section 5(b)) If County terminates other than for cause, County is obligated to pay any disconnection, early cancellation, etc. charges paid by TNS to third parties due to such cancellation. (Section 5(c))
Indemnification	- TNS indemnifies County for IP infringement, provided not caused by County or County's equipment and County has not modified services in unauthorized manner. (Section 6(c)). - If County permits third parties to access services (in this case, County's contractor, Designa, will be the entity using license to service), County must indemnify TNS for all liability arising from third party claims to the extent arising in connection with the Services; however, County's obligation to indemnify TNS shall not apply to: (a) claims that arise from the violation of any federal, state or local law, regulation or ordinance by TNS, (b) claims that arise from a material breach of this Agreement by TNS, (c) indemnification covered under intellectual property infringement terms whereby TNS would indemnify County, or (d) claims for direct damages to real or tangible personal property, or for bodily injury or death proximately caused by TNS's negligence. (Section 2(d)) - County's indemnification obligations capped at 768.28 limits (Section 9(h))
Limitation of Liability	Except for intellectual property infringement, TNS's liability to County on accounts of acts or omissions relating to the Agreement is limited to an aggregate amount to not exceed the amount paid by County during the six (6) months preceding the month in which the cause of action arose. There is no carveout for Public Records. Exceptions to limitation of liability: direct damages for personal injury, property damage, death, gross negligence or willful misconduct. (Section 7(b))
PCI Compliance	- This Agreement obligates County to comply with PCI requirements and technical specifications (e.g., Section 2); however, County's vendor, Designa, is providing the equipment and performing many of County's obligations under this Agreement. TNS and Designa refused to enter into a tri-party agreement. If Designa fails to perform, County may be liable to TNS. - No more than once per year, at County's written request, TNS will provide their annual PCI-DSS Attestation of Compliance (AOC). (Section 6) - County will be Merchant of Record and must ensure compliance with appropriate FACTA and PCI obligations.

ISSUE	DISCLOSURE & APPLICABLE CONTRACT LANGUAGE
Data and Privacy	TNS may not transmit County data outside US, except permitted to UK, US, Australia, India, Malaysia (Section 8(g))
Fees	\$0.06 per transaction fee payable every month. (Exhibit B) - TNS may increase prices as a result of service requirements that cause increase in equipment provisioning, facility costs, or scope (Section 3(b))
Restatement of fees; Increase in fees	- TNS reserves the right to change prices upon 60 days written notice to County at any time after the 24th month of the initial term, provided that changes in prices will not exceed the lesser of 3% or CPI-U change. (Section 3(d)) - If service is suspended or disconnected due to County's breach, fault, negligence, or omission, and TNS subsequently agrees to reinstate service, County will pay TNS all reasonable costs and expenses incurred in suspending service. (Section 5(c))
Confidentiality	County will retain Public Records rights, but otherwise the TNS Service Agreement and pricing will need to remain confidential (certain information may be redacted to comply with posting requirements for commercial service airports under Florida law).
Audit Rights	County may audit TNS's books and records directly related to services (i) no more than once a year; (ii) at County's sole expense; (iii) respecting TNS's security requirements. (Section 4(d))
Insurance	- Risk Management reviewed and approved TNS's COI. (Exhibit 6) - The insurance provision does not require disclosure of SIR. (Section 9(r))
Choice of Law	Virginia law applies, except that Florida law will govern all matters related to sovereign immunity or public records law. (Section 9(h))
Downtime Credit/ Uptime Guarantees	- TNS gives a refund of their monthly fee for excessive downtime. TNS will provide service credit of 0% to 30% for downtime over a three-month average. (Exhibit 4) - County not entitled to any credit or refund for any period during which access to service was suspended due to County's breach, fault, negligence or omission. (Exhibit 4)