

Master Agreement #: MA 758 2300001384

Contractor: **KEEFE COMMISSARY NETWORK, LLC**

Participating Entity: **STATE OF KENTUCKY**

Master Agreement Terms and Conditions:

1. **Scope:** This addendum covers the Inmate Kiosks and Communications contract led by the State of Nevada for use by state agencies and other entities located in the Participating State/Entity authorized by that State's statutes to utilize State contracts with the prior approval of the State's Chief Procurement Official.

The Commonwealth of Kentucky enters into this agreement for Deposit & Payment Processing Services, Category 2, Inmate Kiosks only for The Kentucky Department of Corrections and The Kentucky Division of Probation and Parole. TABLETS ARE EXCLUDED FROM THIS PARTICIPATING ADDENDUM. The term shall be from execution of the last party through the NASPO expiration date of 12/31/2025. Renewals are based on NASPO renewal options of three (3) additional periods of one (1) year each.

2. **Participation:** This NASPO ValuePoint Master Agreement may be used by all state agencies, institutions of higher institution, political subdivisions and other entities authorized to use statewide contracts in the State of Kentucky. Issues of interpretation and eligibility for participation are solely within the authority of the State Chief Procurement Official.

3. **Primary Contacts:** The primary contact individuals for this Participating Addendum are as follows (or their named successors):

Contractor

Name:	Ken Wright, Vice President-Sales
Address:	Keefe Group-Midwest
Telephone:	314-264-2940-office, 440-759-6134- cell
Email:	KWright@keefegroup.com

Participating Entity

Name:	Jenifer Taylor, KCPM
Address:	200 Mero Street, 5 th Floor, Frankfort KY 40601
Telephone:	502-564-6522
Email:	Jenifer.Taylor@ky.gov

4. PARTICIPATING ENTITY MODIFICATIONS OR ADDITIONS TO THE MASTER AGREEMENT

4.1 Governing Law: This PA shall be governed and construed in accordance with the laws of the Commonwealth of Kentucky per KRS 45A.

4.2 Hosting

The Commonwealth is seeking a vendor who can provide a solution per the RFP requirements. If the vendor is proposing a cloud solution, the Commonwealth prefers the proposed cloud solution to be hosted on either AWS or Azure government cloud platforms. If AWS or Azure government cloud is not proposed, the vendor shall propose a commercial Federal Risk and Authorization Management Program (FedRAMP) - certified or HITRUST Cloud platforms. The proposed solution must accommodate the Commonwealth Office of Technology (COT) oversight that includes an isolated tenant, cloud network access (peering connection) and monitoring solutions.

4.3 Commonwealth Information Technology Policies and Standards

- A. The vendor and any subcontractors shall be required to adhere to applicable Commonwealth policies and standards.
- B. The Commonwealth posts changes to COT Standards and Policies on its [Commonwealth Office of Technology - Home - Commonwealth Office of Technology \(Kentucky\)](#) website. Vendors and subcontractors shall ensure their solution(s) shall work in concert with all posted changes. Vendors or subcontractors that cannot comply with changes must, within thirty (30) days of the posted change, request written relief with the justification for such relief. The Commonwealth may: 1) deny the request, 2) approve an exception to the policy/standard, or 3) consider scope changes to the contract to accommodate required changes. Vendors or subcontractors that do not provide the response within the thirty (30) day period shall be required to comply within ninety (90) days of the change.

4.4 Compliance with Kentucky Information Technology Standards (KITS)

- A. The Kentucky Information Technology Standards (KITS) reflect a set of principles for information, technology, applications, and organization. These standards provide guidelines, policies, directional statements and sets of standards for information technology. It defines, for the Commonwealth, functional and information needs so that technology choices can be made based on business objectives and service delivery. The vendor shall stay knowledgeable and shall provide a solution that works in concert with these standards for all related work resulting from this RFP.
<https://technology.ky.gov/about-the-agency/Pages/kits.aspx>
- B. The vendor and any subcontractors may be required to submit a technology roadmap for any offered solution. Additional roadmaps will be submitted upon request of the Commonwealth. If required, the roadmap shall include, but is not limited to, planned, scheduled and projected product lifecycle dates and historical release/patch or maintenance dates for the technology. In addition, any guidance on projected release/revision/patch/maintenance schedules would be preferred.

4.5 Compliance with Industry Accepted Reporting Standards Based on Trust Service Principles and Criteria

The vendor must employ comprehensive risk and threat management controls based on defined industry standards for service organizations such as ISO AICPA TSP section 100, Trust Services Principles and Criteria. The vendor must annually assert compliance and engage a third-party certification registrar to examine such assertions and controls to provide a Report, such as ISO 9000, ISO 14001, AT101 SOC 2 type 2, on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy, which contains an opinion on whether the

operating controls effectively support the assertions. All such reports, including publicly available reports (i.e. AT 101 SOC 3) shall be made available to the Commonwealth for review.

4.6 System Vulnerability and Security Assessments

The Commonwealth reserves the right to conduct, in collaboration with the vendor, non-invasive vulnerability and security assessments of the software and infrastructure used to provide services prior to implementation and periodically thereafter. Upon completion of these assessments, the Commonwealth will communicate any findings to the vendor for action. Any cost relating to the alleviation of the findings will be the responsibility of the vendor. Mitigations will be subject to re-evaluation after completion. In cases where direct mitigation cannot be achieved, the vendor shall communicate this and work closely with the Commonwealth to identify acceptable compensating controls that will reduce risk to an acceptable and agreed upon level. An accredited third-party source may be selected by the vendor to address findings, provided they will acknowledge all cost and provide valid documentation of mitigation strategies in an agreed upon timeframe.

4.7 Privacy Assessments

The Commonwealth reserves the right to conduct privacy assessments of the collection, use, maintenance and sharing of Commonwealth data by any vendor services, software, and infrastructure used to provide services prior to implementation and periodically thereafter. Upon completion of this assessment, the Commonwealth will communicate any findings to the vendor for action. Any cost relating to the alleviation of the findings will be the responsibility of the vendor. Mitigations will be subject to re-evaluation after completion. In cases where direct mitigation cannot be achieved, the vendor shall communicate this and work closely with the Commonwealth to identify acceptable compensating controls or privacy practices that will reduce risk to an acceptable and agreed upon level. An accredited third-party source may be selected by the vendor to address findings, provided they will acknowledge all cost and provide valid documentation of mitigation strategies in an agreed upon timeframe.

4.8 Privacy, Confidentiality and Ownership of Information

The Commonwealth is the designated owner of all Commonwealth data and shall approve all access to that data. The vendor shall not have ownership of Commonwealth data at any time. The vendor shall not profit from or share Commonwealth data. The vendor shall be in compliance with privacy policies established by governmental agencies or by state or federal law. Privacy notice statements may be developed and amended from time to time by the Commonwealth and will be appropriately displayed on the Commonwealth portal (Ky.gov). The vendor should provide sufficient security to protect the Commonwealth and COT data in network transit, storage, and cache. **All Commonwealth data, including backups and archives, must be maintained at all times within the contiguous United States. All Commonwealth data, classified as sensitive or higher, as defined in Enterprise Standards, must be encrypted in-transit from vendor's network and at rest while stored on vendor's laptops or other portable media devices.**

4.9 EU GDPR Compliance

The Commonwealth of Kentucky requires all vendor contracts to comply to the extent applicable with the European Union's General Data Privacy Regulation [Regulation (EU) 2016/679] (the "GDPR") when the Commonwealth is a "controller" or "processor" of "personal data" from an individual "data subject" located in the European Union, as those terms are defined in the GDPR. The vendor acknowledges and agrees that it is acting as a "processor" of "personal data" for the Commonwealth under this Agreement and that all applicable requirements of the GDPR are incorporated by reference as material terms of this Agreement. The vendor represents and warrants that (1) it is aware of and understands its compliance obligations as a "processor" under GDPR; (2) it has adopted a GDPR compliant data privacy compliance policy/program, a summary of which has been provided to the Commonwealth; (3) it will process "personal data" only in accordance with the Commonwealth's instructions; and (4) with

regard to its obligations under this Agreement, it shall comply with all applicable requirements of the GDPR. Additionally, the vendor may be found liable to the Commonwealth for damages arising from any violation of applicable requirements of GDPR by the vendor in its performance of the services hereunder.

4.10 Data Quality

The vendor shall provide proposed levels of data quality per the following dimensions.

Data Quality is the degree to which data is valid, accurate, complete, unique, timely, consistent with all requirements and business rules, and relevant for a given use. The vendor shall provide data quality definitions and metrics for any data elements. Data has to be of the appropriate quality to address the needs of the Commonwealth of Kentucky. The following dimensions can be used to assess data quality:

- Validity – The data values are in an acceptable format.
- Accuracy – The data attribute is accurate.
- Completeness – There are no null values in a data field.
- Uniqueness – There are no duplicate values in a data field.
- Timeliness – The data attribute represents information that is not out-of-date.
- Consistency – The data attribute is consistent with a business rule that may be based on that attribute itself, or on multiple attributes.
- Adherence to business rules – The data attribute or a combination of data attributes adheres to specified business rules.

4.11 License Agreements

Any proposed software agreements, i.e. license agreement, subscription agreement, end-user license agreement, etc. shall include the following, or similar, language:

“All terms in this agreement/EULA shall be read as applicable only to the extent permitted by Kentucky law and no term in violation of the Kentucky law, inclusive of Kentucky Procurement Law, shall be given effect.”

Any third-party software licenses and cloud resources necessary for the proposed solution may be procured via the Commonwealth’s existing contracts.

4.12 Software Version Requirements

All commercially supported and Commonwealth approved software components such as Operating system (OS), Database software, Application software, Web Server software, Middle Tier software, and other ancillary software must be kept current. In the event that a patch interferes with the solution, the vendor must present a plan for compliance to the Commonwealth outlining the constraints and an appropriate plan of action to bring the solution in to compliance to allow this patch to be applied in the shortest timeframe possible, not to exceed three (3) months, unless otherwise negotiated with the Commonwealth.

4.13 No Surreptitious Code Warranty

The vendor represents and warrants that no copy of licensed software provided to the Commonwealth contains or will contain any Self-Help Code or any Unauthorized Code as defined below. This warranty is referred to in this contract as the "No Surreptitious Code Warranty".

As used in this contract, "Self-Help Code" means any back door, time bomb, drop-dead device, or other software routine designed to disable a computer program automatically with the passage of time or under the positive control of a person other than the licensee of the software. Self-Help Code does not include Software routines in a computer program, if any, designed to permit an owner of the computer

program (or other person acting by authority of the owner) to obtain access to a licensee's computer system(s) (e.g. remote access) for purposes of maintenance or technical support.

As used in this contract, "Unauthorized Code" means any malware designed to permit unauthorized access to disable, erase, or otherwise harm software, equipment, or data; or to perform any other such actions. The term Unauthorized Code does not include Self-Help Code.

In addition, vendor will use up-to-date commercial virus detection software to detect and remove any viruses from any software prior to delivering it to the Commonwealth.

The vendor shall defend the Commonwealth against any claim and indemnify the Commonwealth against any loss or expense arising out of any breach of the No Surreptitious Code Warranty.

4.14 Network Connection Requirements

- A. Vendor shall work with COT to establish any network connections. If a secure site-to-site connection is required, the vendor shall employ a secure site-to-site connection procured by the Agency from COT.
- B. Vendor shall, at COT's discretion, provide appropriate access to enable the Commonwealth to perform additional security measures, such as decryption of the network traffic if required for inspection. If the proposed solution does not have the ability to meet this requirement, the vendor must provide an alternative such as audit reporting of this function.
- C. Vendor should provide notifications to the Commonwealth Service Desk for unplanned outages within fifteen (15) minutes.
- D. Vendor shall notify COT Change Management, through the Commonwealth Services Desk, a minimum of two (2) business days prior to any planned outage.
- E. Vendor, in conjunction with the agency, shall provide a Business Impact Assessment (BIA) to appropriately classify all data before production/go-live.
- F. Vendor shall include a Web Application Firewall when application houses any data classified as sensitive or higher as defined in KITS standards.
- G. Vendor shall provide Recovery Time Objective (RTO) and Recovery Point Objective (RPO) services. Vendor shall provide those services to achieve those SLAs.

4.15 OS Requirements

- A. Non-On Prem Solutions
 - 1. No Commonwealth data shall be co-mingled with another entity, without the prior approval of the Commonwealth.
 - 2. Vendor shall provide a solution to move data to the Commonwealth, if required by the Commonwealth.
 - a. At the end of the contract, the vendor shall provide all agency data in a useable standard data format (such as ascii, csv, etc.) that can be converted to a subsequent system. The vendor shall cooperate to this end with the agency and/or a vendor of the agency's choice, in a timely and efficient manner.
 - b. Vendor shall address the destruction of Commonwealth data as defined in CIO-092 and provide a certification of the complete and permanent deletion the Commonwealth data.

B. Infrastructure as a Service

1. Vendor shall work with the agency and COT to establish all administrative personnel engagements.
2. Vendor shall meet certification requirements for classification of data being stored.
3. Vendor shall, at COT's request, provide appropriate access to enable the Commonwealth to perform additional security measures in compliance with Commonwealth Enterprise Policies, Standards, and/or any Federal or State requirements.
4. Vendor shall provide an Exit Strategy, to move all data to the Commonwealth Data Center, if required by the Commonwealth.
 - a. At the end of the contract, the vendor shall provide all agency data in a form that can be converted to any subsequent system of the agency's choice. The vendor shall cooperate to this end with the vendor of the agency's choice, in a timely and efficient manner.

4.16 Project Governance

Vendor shall work with the agency and appropriate COT offices, when needed, in the cases of data governance, security aspects, hosting, integration, etc., provided that such work does not expand the scope of the services as described in Section 50 of this RFP absent a corresponding change order agreed to by the parties reflecting such expansion.

4.17 Monitoring Requirements for On Premise and Cloud (SaaS)

Vendor shall work with the agency and COT to establish a monitoring solution. Vendors shall provide a view into their environment either by providing a COT approved comprehensive dashboard or allow COT to install their KITS compliant monitoring solution; to include but not limited to performance and availability.

4.18 Application and Service Requirements

Current Enterprise Applications and Services

1. COT provides a number of Enterprise Shared Services to State agencies. Vendor shall use published IT Applications and Services provided on KITS for: Enterprise Service Bus, Enterprise Content Management, Data Warehousing, Data Analytics and Reporting, Business Intelligence, Web Services, GIS, unless explicitly approved by COT.
2. Vendor provided dedicated application components (i.e., Application Servers, Databases, etc.) shall comply with KITS or if the technology is not included in KITS, the technology must be accepted by the Commonwealth for inclusion in KITS or granted a written exception to KITS according to COT Information Technology Standards Policy currently CIO-051.
3. Vendor applications must describe in detail all available features and functionality accessible via APIs.
4. All business applications must support the ability to use modern authentication for authentication and authorization. Modern authentication technologies would include SAML 2.0, WSFED, OAuth, or OpenID Connect.

4.19 Project Management Requirements

The COT Division of Governance and Strategy (COT-DGS) is responsible for overseeing large and complex technology projects throughout the Commonwealth. The vendor shall adhere to Project Management standards and reporting requirements established by COT-DGS, which are posted at <https://technology.ky.gov/services-and-support/Pages/About-the-Project-Management-Branch.aspx>. These include, but are not limited to, having a documented project schedule, risk management, issue management and reporting project status to the CIO monthly in the format defined by COT-DGS.

4.20 Applicable Security Control Framework Compliance

The vendor must have an awareness and understanding of the NIST Special Publication 800-53 Security Control Framework and employ safeguards that meet or exceed the moderate level controls as defined within the standard. The vendor must provide sufficient safeguards to provide reasonable protections around the Commonwealth's data to ensure that the confidentiality, integrity, and availability is maintained at an appropriate level. These include but are not limited to:

- *Access Control*
The vendor must employ policy and process that provide for stringent control to limit physical and logical access to systems that house Commonwealth data, on a need to know basis, provide clear separation of duties, and adheres to least privilege principles.
- *Awareness and Training*
The vendor must provide the appropriate role specific training for staff to ensure that there is awareness and understanding of roles and responsibilities as they relate to the protections around the Commonwealth's data.
- *Audit and Accountability*
There must be sufficient auditing capability to ensure that actions are tracked and there is individual accountability for all actions taken by vendor staff.
- *Configuration Management*
The vendor must work within established baselines that provide minimal functionality needed to ensure service delivery without exposing unnecessary risk. The vendor must also employ structured change control processes that provide a level of coordination with the client agreed upon in a Service Level Agreement (SLA).
- *Contingency Planning*
The vendor must employ contingent planning policy and procedures that ensure service delivery based on agreed SLA levels while maintaining all Commonwealth data within the continental United States.
- *Identification and Authorization*
The vendor must employ appropriate identity and access management policies and procedures to ensure that access is appropriately authorized and managed at a level to ensure that access is provisioned and de-provisioned in a timely and efficient manner.
- *Incident Response*
The vendor must employ policy and procedures to ensure that an appropriate response to all identified security incidents are addressed in a timely manner and are reported to the appropriate parties in an agreed upon SLA timeframe. The vendor must also ensure that all staff are sufficient trained to ensure that they can identify situations that are classified as security incidents.
- *Maintenance*
The vendor must employ policy and procedures that ensure that all maintenance activities are conducted only by authorized maintenance staff leveraging only authorized maintenance tools.
- *Media Protection*
The vendor must employ policy and procedure to ensure that sufficient protections exist to protect Commonwealth data on all storage media throughout the media lifecycle and maintain documentation from media creation through destruction.
- *Physical and Environmental Controls*
The vendor must employ physical and environmental policies and procedures that ensure that the service and delivery infrastructure are located in a physically secure and environmentally protected environment to ensure the confidentiality, integrity, and availability of Commonwealth data.
- *Personnel Security*
The vendor must employ policies and procedures to ensure that all staff that have access to systems that house, transmit, or process Commonwealth data have been appropriately vetted and have been through a background check at the time of hire and periodically thereafter.

- *System and Communications Protections*

The vendor must employ physical and logical protection that protect system communications and communication media from unauthorized access and to ensure adequate physical protections from damage.

4.21 Bidder, Offeror, or Contractor Mandatory Representations Compliance with Commonwealth Law

The contractor represents that, pursuant to [KRS 45A.485](#), they and any subcontractor performing work under the contract will be in continuous compliance with the KRS chapters listed below and have revealed to the Commonwealth any violation determinations within the previous five (5) years:

[KRS Chapter 136](#) (CORPORATION AND UTILITY TAXES)

[KRS Chapter 139](#) (SALES AND USE TAXES)

[KRS Chapter 141](#) (INCOME TAXES)

[KRS Chapter 337](#) (WAGES AND HOURS)

[KRS Chapter 338](#) (OCCUPATIONAL SAFETY AND HEALTH OF EMPLOYEES)

[KRS Chapter 341](#) (UNEMPLOYMENT COMPENSATION)

[KRS Chapter 342](#) (WORKERS' COMPENSATION)

4.22 Boycott Provisions

If applicable, the contractor represents that, pursuant to [KRS 45A.607](#), they are not currently engaged in, and will not for the duration of the contract engage in, the boycott of a person or an entity based in or doing business with a jurisdiction with which Kentucky can enjoy open trade. **Note:** The term Boycott does not include actions taken for bona fide business or economic reasons, or actions specifically required by federal or state law.

If applicable, the contractor verifies that, pursuant to KRS 41.480, they do not engage in, and will not for the duration of the contract engage in, in energy company boycotts as defined by KRS 41.472.

4.23 Lobbying Prohibitions

The contractor represents that they, and any subcontractor performing work under the contract, have not violated the agency restrictions contained in [KRS 11A.236](#) during the previous ten (10) years, and pledges to abide by the restrictions set forth in such statute for the duration of the contract awarded.

5. Orders:



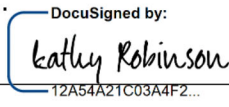
Any order placed by a Participating Entity or Purchasing Entity for a product and/or service available from this NASPO Master Agreement shall be deemed to be a sale under (and governed by the prices and other terms and conditions) of the NASPO Master Agreement unless the parties to the order agree in writing that another contract or agreement applies to such Order

6. Pricing:

VENDOR NAME: Keefe Commissary Network, LLC d/b/a Access Corrections						
Type of Service	CASH Transaction Fee	Commission Rate (10%)	Total Fee CASH	Debit/Credit Transaction Fee	Commission Rate (10%)	Total Fee Credit/Debit
Adult Institutions						
Phone						
EFT - Deposits of \$0.01 - \$50.00		\$ -	\$ -	\$ 2.68	\$ 0.27	\$ 2.95
EFT - Deposits of \$50.01 - \$100.00		\$ -	\$ -	\$ 4.50	\$ 0.45	\$ 4.95
EFT - Deposits of \$100.01 - \$200.00		\$ -	\$ -	\$ 5.41	\$ 0.54	\$ 5.95
EFT - Deposits over \$200.00		\$ -	\$ -	\$ 6.32	\$ 0.63	\$ 6.95
Internet						
EFT - Deposits of \$0.01 - \$50.00		\$ -	\$ -	\$ 1.77	\$ 0.18	\$ 1.95
EFT - Deposits of \$50.01 - \$100.00		\$ -	\$ -	\$ 3.59	\$ 0.36	\$ 3.95
EFT - Deposits of \$100.01 - \$200.00		\$ -	\$ -	\$ 4.50	\$ 0.45	\$ 4.95
EFT - Deposits over \$200.00		\$ -	\$ -	\$ 5.41	\$ 0.54	\$ 5.95
Walk-In (Retail)						
EFT - Deposits of \$0.01 - \$50.00	\$ 2.27	\$ 0.23	\$ 2.50	\$ 2.27	\$ 0.23	\$ 2.50
EFT - Deposits of \$50.01 - \$100.00	\$ 2.27	\$ 0.23	\$ 2.50	\$ 2.27	\$ 0.23	\$ 2.50
EFT - Deposits of \$100.01 - \$200.00	\$ 2.27	\$ 0.23	\$ 2.50	\$ 2.27	\$ 0.23	\$ 2.50
EFT - Deposits over \$200.00	\$ 2.27	\$ 0.23	\$ 2.50	\$ 2.27	\$ 0.23	\$ 2.50
Lobby Kiosk						
EFT - Deposits of \$0.01 - \$50.00	\$ 0.91	\$ 0.09	\$ 1.00	\$ 1.82	\$ 0.18	\$ 2.00
EFT - Deposits of \$50.01 - \$100.00	\$ 0.91	\$ 0.09	\$ 1.00	\$ 3.64	\$ 0.36	\$ 4.00
EFT - Deposits of \$100.01 - \$200.00	\$ 0.91	\$ 0.09	\$ 1.00	\$ 4.55	\$ 0.45	\$ 5.00
EFT - Deposits over \$200.00	\$ 0.91	\$ 0.09	\$ 1.00	\$ 5.45	\$ 0.55	\$ 6.00

Type of Service	CASH Transaction Fee	Commission Rate (10%)	Total Fee CASH	Debit/Credit Transaction Fee	Commission Rate (10%)	Total Fee Credit/Debit
Probation & Parole*						
Lobby Kiosk						
EFT - Payment of Drug Testing or SOTP Fee of \$10.00	\$ 1.00	No Commission	\$ 1.00	\$ 1.00	No Commission	\$ 1.00
EFT - Payment of Drug Testing or SOTP Fee of \$10.01 - \$50.00	\$ 1.00	No Commission	\$ 1.00	\$ 2.00	No Commission	\$ 2.00
EFT - Payment of Drug Testing or SOTP Fee of \$50.01 and over	\$ 1.00	No Commission	\$ 1.00	\$ 4.00	No Commission	\$ 4.00
Phone						
EFT - Payment of Drug Testing or SOTP Fee of \$10.00				\$ 1.95	No Commission	\$ 1.95
EFT - Payment of Drug Testing or SOTP Fee of \$10.01 - \$50.00				\$ 2.95	No Commission	\$ 2.95
EFT - Payment of Drug Testing or SOTP Fee of \$50.01 and over				\$ 4.95	No Commission	\$ 4.95
Internet						
EFT - Payment of Drug Testing or SOTP Fee of \$10.00				\$ 1.00	No Commission	\$ 1.00
EFT - Payment of Drug Testing or SOTP Fee of \$10.01 - \$50.00				\$ 1.95	No Commission	\$ 1.95
EFT - Payment of Drug Testing or SOTP Fee of \$50.01 and over				\$ 3.95	No Commission	\$ 3.95
Walk-In (Retail)						
EFT - Payment of Drug Testing or SOTP Fee of \$10.00	\$ 2.50	No Commission	\$ 2.50	\$ 2.50	No Commission	\$ 2.50
EFT - Payment of Drug Testing or SOTP Fee of \$10.01 - \$50.00	\$ 2.50	No Commission	\$ 2.50	\$ 2.50	No Commission	\$ 2.50
EFT - Payment of Drug Testing or SOTP Fee of \$50.01 and over	\$ 2.50	No Commission	\$ 2.50	\$ 2.50	No Commission	\$ 2.50
Note: For the Walk-in (Retail), debit card transactions are available at the 582 Dollar General locations in the state of Kentucky and the 16,000+ locations throughout the U.S.						

IN WITNESS, WHEREOF, the parties have executed this Addendum as of the date of execution by both parties below.

Participating Entity: Commonwealth of Kentucky Department of Corrections (DOC)	Contractor: Keefe Commissary Network LLC dba Access Corrections (Keefe Group)
Signature: 	Signature: 
Name: Hilarye Dailey	Name: John Puricelli
Title: Deputy Commissioner	Title: Executive Vice President
Date: 6/14/23	Date: 06/12/2023
Participating Entity: Commonwealth of Kentucky Office of Procurement Services (OPS)	
Signature: 	
Name: Kathy Robinson	
Title: Executive Director	
Date: 6/20/2023	

***[Please email fully executed PDF copy of this document to
PA@naspo.valuepoint.org
to support documentation of participation and posting in
appropriate data bases.]***