BUREAU OF THE
Fiscal Service
U.S. DEPARTMENT OF THE TREASURY

February 7th, 2025

FINANCIAL AGENT SOLICITATION
GENERAL LOCKBOX

I. INTRODUCTION

The Bureau of the Fiscal Service (Fiscal Service) plans to select one financial institution to operate, maintain, and improve the Federal government's General Lockbox. Interested financial institutions should respond as specified in Sections VII and VIII of this solicitation.

Fiscal Service will conduct the selection pursuant to its Financial Agent Selection Process (FASP). The financial institution selected shall be a financial agent (FA) of the United States and will have a fiduciary responsibility to act in the best interests of Fiscal Service, including a duty of loyalty and fair dealing. Fiscal Service will expect full transparency in all dealings with the FA, including all communications and pricing.

Fiscal Service will evaluate the Proposals submitted by financial institutions in two phases. In Phase I, Fiscal Service will review all the Proposals and select up to four finalists. In Phase II, each finalist will receive additional detailed information and present their final proposal, and Fiscal Service will select one of the finalists as FA.

Fiscal Service will enter into a 4-year financial agency agreement (FAA) with the FA. Fiscal Service will have the option to extend the FAA for two additional 2-year terms, and two 1-year terms for a maximum possible term of ten (10) years.

The FA may use third-party contractors to assist in providing the services required in the FAA. Any third-party vendors must be approved by Fiscal Service.

LEGAL AUTHORITY

Pursuant to its legal authorities, including 12 U.S.C§§ 90 and 265, 31 U.S.C. §§ 3301 and 3302, and 31 CFR Part 202, Fiscal Service is authorized to designate a Financial Agent for the purpose of providing lockbox collection and remittance services. Financial agents have the fiduciary responsibility to act on behalf of, and in the best interest of, the Government during the performance of their duties under an agent-principal relationship with Treasury. In order to be eligible for designation as a Financial Agent, financial institutions must meet the requirements set forth in 31 C.F.R. Part 202. Notwithstanding this limitation, financial institutions may contract with other service providers including non- financial institutions such as financial technology companies (fintechs) to provide the services solicited in this document. The application must be submitted by the financial institution who will have the legal relationship with Fiscal Service and liability and responsibility to Fiscal Service for any services provided by contractors.

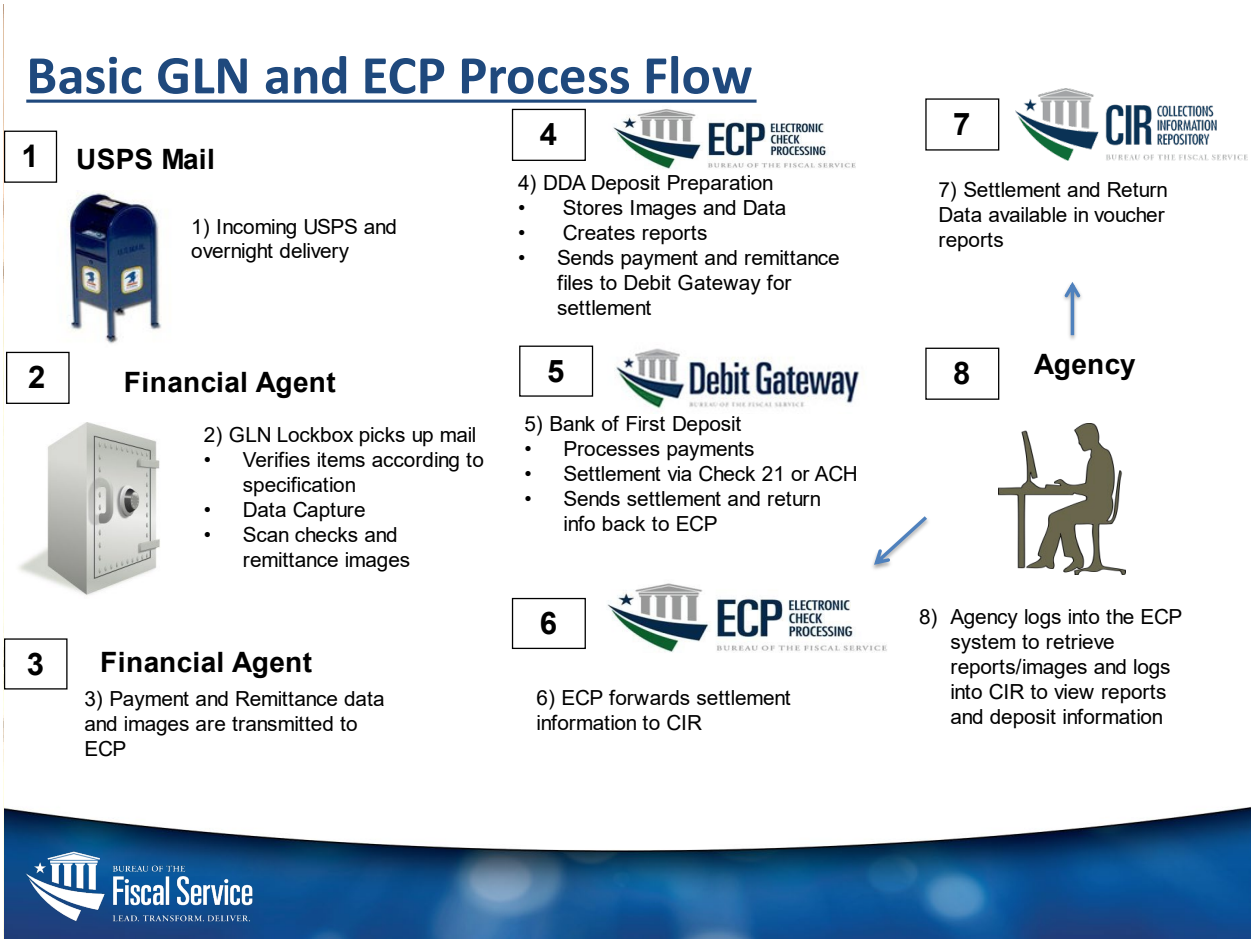
II. BACKGROUND

A. General Lockbox Network (GLN)

The GLN currently is comprised of one FA that provides lockbox collection and remittance services for non-tax collections to Fiscal Service on behalf of Federal agencies. The current FA uses two sites with approximately 12,000 sq. ft at each site. Agencies instruct remitters to mail payments directly to P.O. boxes. The FA collects and sorts the mail, opens envelopes and extracts the contents, captures required check and remittance data and images, processes the financial and remittance data against a set of business rules, balances the day's work, transmits the collected check and remittance data to our Electronic Check Processing (ECP) system, and in some cases transmits the remittance and deposit data to the agencies.

The GLN currently manages approximately 130 lockboxes for 53 government entities. In FY 2024, the GLN processed 16 million items and collected a total of $12.5 billion, with 94% of that volume being checks.

Each individual agency cashflow follows a Statement of Required Services (SRS) which defines the work activities, deliverables, and collection services to be provided by the FA. Copies of all SRS documents will be provided.



There are two basic types of GLN services available to Federal agencies:

Retail Lockbox

The retail lockbox is generally for high volume remittance collections processing. The FA will collect mail, transport it to a lockbox facility and process and deposit receivables. High-speed image scanning equipment reads, verifies, and captures remittance data from the machine-readable remittance documents using optical character recognition (OCR) technology. Remittance data is captured and transmitted to ECP and potentially the agency.

Wholesale Lockbox

The wholesale lockbox is generally for more complex remittances. The FA will collect mail, transport it to a lockbox facility and process and deposits receivables. Although various technologies may be used, these items usually do not include a standardized payment coupon, but may require data capture, document preparation, and sorting rules. This line of business requires more manual effort and/or detailed processing. The FA will work closely with the agency customers to comply with their requirements, which may include non-standard lockbox services such as complex manual processes or interaction with agency's internal systems.

In FY24, 52% of the check payments (7.85 million items), 77% of the card payments (660 thousand items) and 70% of the correspondence (160 thousand items) were classified by the current provider as wholesale. Please review each SRS carefully for more information about processing instructions required by each cashflow.

B. Objectives

Fiscal Service is seeking one FA that can support the GLN in achieving the following business objectives:

- Competition between Financial Institutions – By holding an open competition for services, we expect to identify the most qualified FA that can provide the highest level of service at the best commercially reasonable prices.

- Provide a Stable, Secure, and Scalable Operating Environment – Fiscal Service expects to find a stable, secure, and scalable operating environment for General Lockbox Services. Stable means at least 99% uptime availability; Secure means that the agent meets or exceeds all Fiscal Service (Physical, Personnel, and IT) security requirements; Scalable means an ability to manage volumes rapidly.

- High Quality Program Management – Fiscal Service expects to partner with an FA having extensive industry experience that provide technically skilled experienced employees with a proven track record of exceptional operations and superior customer service. The FA team should include a diverse mix of skill sets that correspond to major aspects of financial transaction processing, including IT development, operations, project management, efficiency analyses, security, and customer service. The FA team should also demonstrate the experience and ability to work cohesively with potential competitors to accomplish the Bureau of Fiscal Service's operational and strategic goals.

- Industry and Technology Expertise – In this specialized business line, an FA with both technical and industry experience and certifications will best position the General Lockbox for success, security, stability, and redundancy. The FA will keep abreast of developments in financial transaction processing and offer advice regarding best-in-class technical changes and innovative solutions. The FA will demonstrate a track record of reliability in meeting operational metrics and system availability.

- Innovation and Process Improvement – Fiscal Service seeks an FA that can identify innovative solutions and process improvement to support major initiatives by increasing efficiencies to control or reduce cost. Please provide your suggestions for automating wholesale processing to a more standard process such as retail. The selected FA will demonstrate their ability to meet these expectations in their response to the FASP, as well as be required to provide a written plan for driving innovation/efficiencies and managing/reducing costs on an annual basis throughout the term of the FAA.

- Ensure Operational Continuity and Satisfy Critical Transition Dates – If the current provider is not selected, the newly designated FA will be responsible for transitioning all cashflows by April 2, 2027. There is NO flexibility regarding this date.

III. TECHNICAL AND PROCESSING REQUIREMENTS

A. GLN Core Processing Requirements

The FA will provide the following core critical lockbox services to agencies as required by the SRSs for each cashflow. Additional services may be required for particular cashflows.

- Post office box rental
- Lockbox setup
- Mail collection, extraction, batching, and sorting
- Remittance processing
- Check processing
- Credit card processing via Pay.gov
- Data capture
- File creation and transmission (multiple files created and sent on a daily basis) based upon the customer's requirements
- Deposit processes to ECP
- Balancing
- Exception processing
- Various daily and monthly reporting
- Preparing and sending daily outgoing mail packages
- Customer service (including research requests, Check Image review and document review, implementation of customer requests)
- Lockbox closures and mail forwarding
- Billing
- Records safekeeping and destruction

B. Program Resources

The FA will provide staff with expertise in all areas of lockbox processing along with expertise in program and project management, security (Physical, personnel, and IT), customer service, and systems development. The current FA employs 140 individuals, with 119 dedicated to operations and the remaining 21 committed to support functions.

C. Service Level Requirements

The FA will provide the highest standards of performance and quality and must perform ongoing daily quality control reviews of work in process. Fiscal Service will review the established quality controls on an on-going basis to ensure performance meets established standards. This

includes a review of accuracy, work volume accountability, workload tracking, responsiveness, timeliness, system availability, and security.

Fiscal Service performs ongoing quality control reviews using a Metric Tracking System. This Excel-based tracking system is used to track every cashflow and the associated Service Level Agreements (SLAs). Each day the FA will send an Excel file detailing the number of checks processed and dollar amount deposited via ECP by cashflow. Fiscal Service uses the daily files to balance reports sent internally through ECP. Each month the FA will send a more detailed Excel file listing the cashflow types and SLA data for each cashflow. This data is used to evaluate the FA's performance. The format and particulars of the requested data are subject to change. We welcome ideas on how to provide this data in a different – and ideally more automated – format.

Each lockbox site is expected to be open Monday through Friday with the exception of federal holidays. Hours of operation will be based on Continental United States time zones.

D. Lockbox Relationship Management/Customer Service

The FA will provide all aspects of Federal agency customer service. The FA will designate customer service liaisons to receive all agency customer service inquiries and requests by phone, email, and other forms of correspondence and provide research services and program support. The most common customer service request examples include inquiries about delayed packages, Adjustment Correction Rescission (ACR) requests, Payment In Lieu (PIL) requests, system adjustments and drop files.

The customer service hours for each lockbox site are Monday to Friday from 8:00 am – 8:00 pm ET (with the exception of federal holidays) to receive agency customer service requests. The selected FA is required to provide a weekly/monthly summary of each agency request along with the resolution/response. The summary is due no later than 20 days following the period.

Further, the FA is to develop, maintain, and update an agency contact list annually with at least the basic information by agency cash flow/lockbox (Name, Title, Phone Number, and E-Mail Address) and make sure it is available to both the Fiscal Service GLN and Customer Experience teams. In addition, please familiarize yourself with OMB Circular A- Section 280 on CX as enterprise call center metrics and standards are currently being developed and will be expected to be implemented once finalized.

E. Systems Interface

The FA will be required to interface with the following Fiscal Service systems:

Electronic Check Processing (ECP)

The FA will interface with ECP, the Fiscal Service's system to convert paper checks into ACH or Check21 items. The ECP system is a web-based client facing application used by Federal agencies to view transactions for research and reporting purposes. The FA captures images of paper checks and remittance data and transmits files to ECP. The check images and remittance data will be stored in ECP, where they can be viewed by ECP system users as soon as they are received. The FA will transmit the following files to ECP for processing and settlement:

- Item File: Transaction file containing all the financial data related to the transaction. Item file consists of MICR line information, dollar value, and settlement, cashflow, and transaction identification. It is comprised of one or more batches. Each batch is comprised of payments from a single cashflow.
- Check Image File: Check image files relate financial payment information to the actual financial instrument. They contain all the check images in TIFF format (front and back of the check) and the control file.
- Remittance Document Image File: Contains all the electronic remittance images such as a coupon or payment stub and includes a control file. Zip files contain images in TIFF format and control file .xml.
- Control File: Outlines the contents of an image file.
- Remittance Document Information File: Contains the data values from the coupon, payment stub or user defined data (UDD) e.g. invoice number, customer ID, form number etc. to be stored and is associated with a specific remittance document.
- Relationship File: Used to identify the relationship between the Individual Reference Number (IRN) and Remittances.

Pay.gov

Pay.gov is a Fiscal Service system that provides Federal agencies with a secure government-wide portal for collecting funds electronically. The FA will interface with Pay.gov for all credit card and debit card transactions. There are two main Pay.gov services that the FA may utilize to process these transactions. The FA will choose the service that best fits its business model. These services include an interactive web-portal and a non-interactive transaction submission service.

- The Pay.gov Create Transactions service is an online tool used to process credit and debit card transactions as well as ACH debit transactions. The FA's staff is granted access to the application with the proper roles they are assigned. Once authorized agency staff log on, they manually key in transaction information. This information includes the customer's personal information associated with the payment type (plastic card or ACH debit) as well as the required account information.

- The Pay.gov Trusted Collection Services (TCS) allow for programmatic submission of transactions to Pay.gov for processing. TCS enables a secure web services-based connection to Pay.gov. The FA collects all transaction information, and the data is submitted to Pay.gov via TCS. Submission of data is sent to Pay.gov in a single transaction or as a batch of transactions.

The FA must maintain Plastic Card Industry (PCI) compliance and submit all PCI compliance paperwork to Fiscal Service.

Bank Management System (BMS)

BMS is the system used by Fiscal Service to review, approve, and pay expenses incurred by its financial agents. The FA will report its expenses each month through BMS.

IV. INFORMATION SECURITY REQUIREMENTS

The Financial Agent's performance and systems shall comply with applicable federal government laws, directives, executive orders, standards, guidelines, and other requirements for information security, personnel security, physical security, and data encryption. The Financial Agent's performance and systems shall comply with the most current versions of the following applicable Federal and industry information technology regulatory requirements and standards:

- Fiscal Service Baseline Security Requirements (BLSRs)
- FIPS 140, Security Requirements for Cryptographic Modules
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
- NIST Cybersecurity Framework
- NIST Privacy Framework
- NIST SP 800-37
- NIST SP 800-53
- NIST SP 800-53A
- NIST SP 800-63-3
- NIST SP 800-137
- NIST SP 800-171
- OMB Circular A-123
- OMB Circular A-130
- Public Law 93-579, The Privacy Act of 1974
- IRS Publication 1075
- TD P 85-01 - Treasury Information Technology Security Program

- TD P 15-71 - Department of the Treasury Security Manual
- Payment Card Industry Data Security Standard (PCI DSS)
- SSAE 18 or equivalent
- CISA Binding Operational Directives and Emergency Directives

New regulatory requirements and standards shall be adhered to as they are enacted or become effective, as applicable. The Financial Agent shall implement a process to support timely compliance with new requirements imposed by external authorities.

The Financial Agent employees, facilities, services and product(s) shall meet applicable federal government laws, directives, executive orders, standards, guidelines, and other requirements for information security, personnel security, physical security, and data encryption. The Financial Agent shall follow United States Government, Treasury, and Fiscal Service procedures for proper handling of Controlled Unclassified Information (CUI) and Personally Identifiable Information (PII). The Financial Agent may be required to assist with security reviews by providing information about processes, software, facilities, personnel, and equipment through interviews, on-site inspections (if necessary), and documentary evidence.

CUI, data, and/or equipment will only be disclosed to authorized personnel on a need-to-know basis. The Financial Agent shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. When no longer required, this information, data, and/or equipment will be returned to Government control, destroyed, or held until otherwise directed. Destruction of items shall be accomplished by following NIST Special Publication 800-88, Guidelines for Media Sanitization.

Work shall be performed on systems secured at least at a FIPS 199 MODERATE security category level.

Systems and services placed on the Fiscal Service portfolio must be authorized as per Fiscal Service Security Assessment & Authorization (SA&A) and Information Security Continuous Monitoring (ISCM) policies. Cryptographic modules used to protect Fiscal Service information must be compliant with the current FIPS 140 version. Encryption is required to protect federal and contractor data when transmitting between systems.

Cloud based systems or services shall comply with OMB Federal Risk and Authorization Management Program (FedRAMP) requirements, as well as FedRAMP Privacy requirements. These requirements are in addition to U.S. Government, Department of the Treasury, and Fiscal Service requirements specified throughout this document. Cloud Service Providers shall have FedRAMP compliant security documentation sufficient to obtain a provisional authorization. Fiscal Service Cloud based systems must utilize Treasury TIC services.

V. OVERALL FASP FORMAT

The General Lockbox FASP will be broken into two phases.

The first phase will focus on the financial institution's experience and capability to deliver lockbox services at this scale, commitment to follow Fiscal Service Security Requirements, recommendations for innovation and enhancements, commitment to integrate with ECP, Pay.Gov, and BMS, commitment to sign the core Financial Agency Agreement (FAA), rationale and explanation for the proposed lockbox technology, redundancy, and site locations, and commitment to provide services defined in each cashflow's Statement of Required Services. Following the written Phase I proposal, each financial institution will be scheduled for an in-person briefing covering the contents of their proposal. The oral presentation/briefing will provide an opportunity for us to ask questions and ensure there is no miscommunication or misunderstanding regarding the written proposal.

The second phase will also require a written proposal which will focus on pricing, the ability and plan to control costs and drive efficiencies, and your transition plan (and associated transition pricing). Like Phase I, each financial institution will be scheduled for an in-person briefing covering the contents of their Phase II proposals. The oral presentation/briefing will provide an opportunity for us to ask questions and ensure there is no miscommunication or misunderstanding regarding the written proposal.

Prior to each phase, Fiscal Service will host an information session to provide more details and answer questions.

VI. PRE-FASP

For those financial institutions interested in responding, the pre-FASP requirements are:

- Submit a letter of intent to respond to the GLN FASP on official letterhead signed by the appropriate officer of your bank.
- Along with the above letter, please provide signed Non-Disclosure Agreements (NDA) for those in your organization that will be working to respond to the GLN FASP (See Appendix XIII for the NDA).
- RSVP for the initial Information Session to GLN2025FASP@fiscal.treasury.gov. A maximum of 4 representatives will be accepted from each financial institution. Signed NDAs will be required for the Information Session.
- Phase I Information Session: An in-person information session will be held in Washington, DC on February 20th, 2025 starting at 9:30am. The session will cover a summary of the entire FASP, and we will provide detailed information on requirements for Phase I proposals including specifics surrounding security and audit requirements, the core Financial Agency Agreement (FAA), how to interface with ECP, Pay.gov, and

BMS, and Statements of Required Services. Details regarding in-person briefings of proposals will be covered at the information session.

VII. RESPONSES FOR PHASE I

Proposal Format Requirements

Proposal documents should not be marked as *"Proprietary and Confidential"* and Fiscal Service will not honor any such markings. However, because Proposals may be subject to Freedom of Information Act (FOIA) requests, Congressional inquiries, or other requests, Proposal documents may be labelled as *"Program Sensitive"* to emphasize concerns about the disclosure of confidential business information.

Proposals should not contain, and the Fiscal Service will not consider, information on pricing and program costs. Fiscal Service will request pricing information from finalists in Phase II of the evaluation process.

Format Specifications: Proposals must be formatted as follows:

- No more than 30 one-sided pages (not including any requested attachments)
- Appendix- no more than 10 pages
- Paper size 8 ½" x 11"
- Single-spaced
- Font type and size – 12-point Times New Roman font
- Margin size – one inch
- A table of contents is optional (not included in 20-page maximum)
- 11 paper copies of the Proposal
- Adobe PDF format of the proposal and transmittal letter

Transmittal Letter: Proposals must include a transmittal letter as follows:

- The transmittal letter must be written on the financial institution's letterhead and be signed by an official of the financial institution with legal authority to represent and bind the institution.
- The transmittal letter must include the name, title, mailing address, e-mail address, and telephone number of the financial institution's contact person for all communications related to the FASP.
- The financial institution must affirmatively state in the transmittal letter that it (1) qualifies as a financial agent under 31 CFR Part 202; (2) agrees to the selection and evaluation approach described in this solicitation; and (3) understands that the selection is subject to the Fiscal Service's FASP and is not subject to the Federal Acquisition Regulation (FAR).

Submission: Financial institutions should submit their PDF formatted response to GLN2025FASP@fiscal.treasury.gov by 5:00 pm ET on April 4, 2025. Paper versions should be sent by courier or traceable delivery service to:

Mrs. Erika Bevins
GLN Branch Manager
U.S. Department of the Treasury
Bureau of the Fiscal Service
401 14th Street, SW, Room 412D
Washington, DC 20227

Questions about the Solicitation: Outside of the information sessions, financial institutions should direct all questions about this solicitation to the following email mailbox address: GLN2025FASP@fiscal.treasury.gov. Fiscal Service will respond to all questions in writing via e-mail as soon as possible and may share questions and answers with other respondent financial institutions.

Phase I Proposal Details

To recap, Phase I will focus on the financial institution's experience and capability to deliver lockbox services at this scale, commitment to follow Fiscal Service Security Requirements, recommendations for innovation and enhancement, commitment to integrate with ECP, Pay.Gov, and BMS, commitment to sign the core Financial Agency Agreement (FAA), a rationale and explanation for the proposed lockbox technology, redundancy, and site locations, and commitment to provide services defined in each cashflow's Statement of Required Services. Proposals should clearly demonstrate the financial institution's ability to meet the related Objectives in Section B., along with the ability to address requirements in Section III, *Technical and Processing Requirements.* At a minimum, Phase I proposals should describe the following:

- Experience, both corporate and staff that will be assigned, with retail and wholesale lockbox processing.
- Explanation regarding staffing methodology (temporary vs permanent) and how those positions will be filled,
- How you plan to meet customer service requirements.
- Rationale for proposed site locations.
- Rationale for proposed technology and equipment platforms.
- Proposal for a 21st century lockbox including ideas for innovation.
- Recommendations regarding processing over-the-counter type deposits received via mail.
- Plans for redundancy and disaster recovery including recovery times.
- Commitments to follow Bureau security requirements.

- Commitments to interface with ECP, Pay.Gov, and BMS.
- Commitment to terms in the core FAA
- Any other relevant information to assist Fiscal Service in evaluating the Phase I proposal.

VIII. PHASE I EVALUATION AND SCORING

After all of the submitting financial institutions' in-person briefings are completed, Fiscal Service will evaluate and score all Phase I Proposals and invite up to four (4) financial institutions with the highest scores to proceed to Phase II as finalists. The selection of those highest scoring proposals is at the sole discretion of Fiscal Service. Fiscal Service will notify those financial institutions below the top 4 scores that they will not be moving on to Phase II of the FASP.

IX. PHASE II INFORMATION

Fiscal Service will conduct a Phase II information sessions for all finalists. The Phase II session will provide detailed information regarding information and materials regarding the pricing template, transition plan, and efficiency and cost management requirements, along with how to respond with Phase II proposals.

Additional information sessions consisting of open dialogue with Fiscal Service, both with individual finalists and collectively with all finalists, may occur at the discretion of Fiscal Service. Fiscal Service will provide all finalists with the opportunity to ask questions and to clarify the terms of their Proposals throughout the evaluation process.

Like Phase I, each finalist will be invited to present its final Phase II Proposal in an oral presentation held in person at Fiscal Service headquarters in Washington, DC. After the oral presentations, Fiscal Service will select one finalist as the FA for the GLN. The FA will be required to execute the FAA with Fiscal Service within approximately 3 months after the date it is notified of its selection.

X. FASP TIMELINE

The table below is the current timeline. Please note that while we will make our best efforts to adhere to these dates, there may be circumstances that force date changes. We will provide sufficient notice if this occurs.

GLN FASP Event	EXPECTED START	EXPECTED END
Publish GLN FASP	February 7, 2025	
GLN FASP Information Session	February 20, 2025	
Phase I Proposals Due	April 4, 2025	
Phase I Oral Presentations	Week of 4/28/2025 or 5/5/2025	
Notify FIs – Non-Selection or Advance to Phase II. Provide Phase II Documentation	Early May 2025 (TBD)	
Phase II Information Session	Late May 2025 (TBD)	
Phase II Proposals Due	July 2025 (TBD)	
Phase II Oral Presentations	July – August 2025 (TBD)	
Final Negotiations – 8 Weeks	August 2025	October 2025
Sign FAA	10/31/2025	

This financial agent solicitation may be amended from time to time, or cancelled in its entirety, in the sole discretion of Fiscal Service.

Don M. Linder

Digitally signed by Don M. Linder
Date: 2025.02.06 07:35:51 -05'00'

D. Michael Linder Date
Assistant Commissioner, Revenue Collections Management
Bureau of the Fiscal Service
U.S. Department of Treasury

XI. APPENDIX

- Non-Disclosure Form
- Attachment A

NON-DISCLOSURE AGREEMENT
Between
U.S. Department of the Treasury, Bureau of the Fiscal Service,
and _____

WHEREAS, the U.S. Department of the Treasury, Bureau of the Fiscal Service ("Fiscal Service") is currently soliciting proposals from commercial banks for the operation of a General Lockbox Program;

WHEREAS, _____ ("Bank") has expressed a prospective interest to Fiscal Service in participating in the General Lockbox Financial Agent Selection Process ("FASP"), and Fiscal Service deems it to be in the Government's best interest to facilitate receipt of a proposal from Bank in connection with the General Lockbox FASP, because increased competition enhances the probability of Fiscal Service selecting an agent whose proposal best meets the Government's needs;

WHEREAS, Bank may, in order to most effectively participate in the General Lockbox FASP require, at the sole discretion of Fiscal Service, access to certain Confidential Information of Fiscal Service for use in connection with the preparation of its proposal;

NOW, THEREFORE, in consideration of the foregoing, and the mutual promises and covenants contained herein, the receipt and sufficiency of which are hereby acknowledged, Fiscal Service and Bank hereby enter into this Non-Disclosure Agreement ("Agreement"), subject to the following terms and conditions:

1. **Confidential Information.** Fiscal Service may, in its sole discretion, disclose to Bank the following documents and information about the Fiscal Service General Lockbox applications, which constitute Confidential Information: source code, documentation such as use cases, screen prints, details of interfaces, application architecture, security, operating procedures, authentication and authorization approaches for General Lockbox, information about shared components of the Treasury Web Application Infrastructure ("TWAI") on which General Lockbox components could potentially reside, platform information and any other Sensitive But Unclassified ("SBU") or Confidential information deemed necessary to disclose during discussions.

   The term "source code" means the complete version of the source codes for current Fiscal Service General Lockbox applications and will include all existing associated material required to enable a reasonably skilled programmer to understand the licensed product's design, structure and implementation. Additional information may include flow charts, system documentation, program procedures (including build procedures), custom or special compiler information and other material related to the structure and implementation of the systems.

2. **No Representation as to Future Work.** Bank expressly acknowledges that it may not be selected as the financial agent pursuant to the General Lockbox FASP, and that any

costs or expenses incurred by it in preparing a proposal shall be borne solely by Bank and are not reimbursable. The execution of this NDA does not guarantee or imply that any such work will be awarded. In addition, the requirements as outlined in the Notice to Financial Institutions, Financial Agent Selection Process For General Lockbox remain subject to change, including cancellation without notice or cause, at any time.

3. **Duty of Confidentiality and Standard of Care.** No right, title, license, or other interest in the Confidential Information is hereby conveyed to Bank. Bank is authorized to review and use the Confidential Information for the limited purpose of developing its proposal in connection with the General Lockbox FASP. Bank shall limit access to the Confidential Information to it and its present or prospective directors, officers, employees, agents, consultants, or advisors (collectively, "Representatives") with a need-to-know such information for the purpose of preparing its proposal for the General Lockbox FASP. Bank and its Representatives shall not use the Confidential Information for any other purpose. This includes, but is not limited to, the use of any ideas, concepts, design and processes embodied in any Confidential Information (including but not limited to source code) provided or developing any derivative works of such Confidential Information for processing transactions for any other entity except the US Treasury. Bank agrees to take all reasonable and necessary steps to protect the confidential status of the information disclosed and agrees to use its best efforts to regain any information that has been inadvertently transmitted to a third party. Bank shall notify all employees, subsidiaries, affiliates, and Representatives to whom any of the Confidential Information is communicated or disclosed of the terms of this Agreement, and in advance of disclosure of the Confidential Information shall enter into nondisclosure agreements with such parties containing terms and conditions substantially similar to those contained herein

4. **No Warranties as to Accuracy and Completeness.** Fiscal Service makes no representation, warranty, assurance, guarantee or inducement to Bank with respect to the Confidential Information's validity, merchantability, accuracy or completeness, or to the infringement of trademarks, patents, copyrights or any other right of privacy, or other rights of third persons. Bank further agrees that Fiscal Service shall have no liability to Bank or to any of its Representatives relating to or resulting from the use of the Confidential Information by Bank or its Representatives.

5. **Equitable Relief.** Bank agrees that a breach of this Agreement would cause immediate and irreparable injury to Fiscal Service, and that money damages would not be a sufficient remedy for breach of the confidentiality obligations of this Agreement. Accordingly, Fiscal Service shall be entitled to specific performance and/or injunctive relief as a remedy for any breach of the confidentiality obligations of this Agreement. Such remedies shall not be deemed to be the exclusive remedies for a breach by Bank or its Representatives of this Agreement but shall be in addition to all other remedies available at law or equity.

6. **Return and Destruction.** Bank shall return hard copies of the Confidential Information and shall certify in writing as to the destruction of any electronic files of the Confidential

Information (including without limitation all notes, extracts, studies, compilations, memoranda and other documents containing such information) to Fiscal Service within five working days of notice of non-selection in the event that Bank is not selected to perform any work pursuant to the General Lockbox FASP.

7. **Termination.** This Agreement shall terminate five (5) years from the effective date hereof. Any earlier termination of this Agreement shall not relieve Bank, its employees, contractors, and representatives of their obligations hereunder regarding the protection and use of Confidential Information set forth in Paragraph 3) above.

8. **Jurisdiction.** This United States District Court of the District of Columbia shall have exclusive jurisdiction and be the appropriate venue with respect to any matter relating or pertaining to this Agreement.

9. **Assignment.** This Agreement may not be assigned or otherwise transferred by Bank, in whole or in part, without the express prior written consent of Fiscal Service, which consent shall not unreasonably be withheld. This Agreement shall benefit and be binding upon the successors and assigns of the parties hereto.

10. **Paragraph Titles**. The paragraph titles contained herein shall not be deemed to be substantive and shall not be interpreted as to limit or restrict the rights and obligations of the parties as provided herein.

11. **Severability and Construction**. In the event that one or more of the provisions of this Agreement is determined to be void or unenforceable by a court of competent jurisdiction, such finding shall have no effect on the remaining provisions. If any provision is found too broad to be effective, that provision shall be limited to the minimum extent necessary and enforced to the maximum extent possible. This Agreement is a product of negotiation between the parties and expresses the mutual intent of the parties. This Agreement shall not be construed against either of the parties based on drafting.

12. **Merger.** This represents the entire Agreement of the parties concerning the exchange of the Confidential Information and supersedes any and all prior written or oral agreements thereon. It shall not be amended or modified except by subsequent agreement in writing and signed by the duly authorized representatives of the parties.

13. **Electronic Signatures**. Electronic signatures may be used in the execution of this Agreement, which, if used, shall be considered binding original signatures."

IN WITNESS WHEREOF, the undersigned represent that they are authorized to bind their respective organizations to the terms of this Agreement and hereby do so.

_____ _____

Michael Mackay Date
Director, Revenue Remittance Management Division
Bureau of the Fiscal Service
U.S. Department of the Treasury

_____ _____

[NAME] Date
[TITLE]
[**Bank's Registered Name**]

Attachment A for FASP

1 Information Types

The term "information" is synonymous with data, regardless of format or medium.

1.1 Sensitive But Unclassified Information

Sensitive But Unclassified information (SBU) is any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act but which has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy. SBU information is subject to stricter handling requirements than less sensitive non-SBU information because of the increased risk if the data are compromised. Some categories of SBU include financial, medical, health, legal, strategic, and business information. Personally Identifiable Information and Sensitive PII are also considered to be SBU. These categories of information require appropriate protection individually and may require additional protection when aggregated with other sensitive information.

1.2 Controlled Unclassified Information

CUI is defined as information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency. Law, regulation, or government-wide policy may require or permit safeguarding or dissemination controls in three ways: Requiring or permitting agencies to control or protect the information but providing no specific controls, which makes the information CUI Basic; requiring or permitting agencies to control or protect the information and providing specific controls for doing so, which makes the information CUI Specified; or requiring or permitting agencies to control the information and specifying only some of those controls, which makes the information CUI Specified, but with CUI Basic controls where the authority does not specify.

1.3 Personally Identifiable Information

Personally Identifiable Information (PII) as defined in OMB Memorandum M-07-16, refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important to recognize that non-PII can become PII whenever additional information that is publicly available — in any medium and from any source — is or can be combined to identify an individual. As an example, PII includes a name and an address because it uniquely identifies an individual, but alone may not constitute PII.

1.4 Sensitive Personally Identifiable Information

Sensitive PII refers to information that can be used to target, harm, or coerce an individual or entity; assume or alter an individual's or entity's identity; or alter the outcome of an individual's or entity's activities. Sensitive PII requires stricter handling because of the increased risk to an individual or associates if the information is compromised. Some categories of Sensitive PII include stand-alone information, such as Social Security numbers (SSN) or biometric identifiers. Other information such as a financial account, date of birth, maiden names, citizenship status, or medical information, in conjunction with the identity of an individual (directly or indirectly inferred), are also considered Sensitive PII. In addition, the context of the information may determine whether it is sensitive, such as a list of employees with poor performance ratings or a list of employees who have filed a grievance or complaint.

2 Information Protection

The Financial Agent's employees, facilities, services and product(s) shall meet applicable United States (U.S.) federal government laws, directives, executive orders, standards, guidelines, and other requirements for information security, personnel security, physical security, and data encryption. The Financial Agent shall follow United States Government, Treasury, and Fiscal Service procedures for proper handling of SBU, CUI and PII. The Financial Agent may be required to assist with security reviews by providing information about processes, software, facilities, personnel, and equipment through interviews, on-site inspections (if necessary), and documentary evidence.

The Financial Agent shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. When no longer required, this information, data, and/or equipment will be returned to Government control, destroyed, or held until otherwise directed.

Security and privacy control documentation shall include an allocation of responsibility between control providers regarding control implementation. The documentation shall also include a description of the security and privacy controls implemented and demonstrated use of a system development lifecycle in the implementation of security and privacy controls. The Financial Agent shall establish processes to identify and address weaknesses or deficiencies in their supply chain. Supply chain controls will be implemented as part of these processes and documented by the Financial Agent.

The disposition of all data will be at the written direction of the Fiscal Service representative, this may include documents returned to Government control; destroyed; or held as specified until otherwise directed. Items returned to the Government shall be hand carried or sent by certified mail to the Fiscal Service representative.

The Financial Agent shall be responsible for properly protecting all information used, gathered, or developed as a result of work under this agreement. The Financial Agent shall also protect all Government data, equipment, etc.

Information systems and services performing work on behalf of the Fiscal Service shall be located, operated and maintained within the U.S.; operations and maintenance of systems shall be conducted by personnel physically located within the U.S or its territories. "Operated" refers to carrying out administrator/privileged user functions, such as, database administration, patching, upgrades and maintenance. Administrator/ privileged access shall not be permitted from outside of the U.S. Foreign remote maintenance, systems monitoring, foreign "call service centers," "help desks," and the like are prohibited. Fiscal Service information shall be accessed only by personnel meeting or surpassing the Treasury citizenship requirements. Extra precautions should be in place for other types of access from foreign locations.

The Financial Agent must not remove SBU, CUI or PII information from approved location(s), electronic device(s), or other container(s), without prior approval from Fiscal Service.

The Financial Agent shall report security incidents to Fiscal Service via the established incident reporting procedure in the FAA, if applicable.

2.1 Privacy Act Compliance

(a) Financial Agents must comply with the Privacy Act's requirements in the design, development, or operation of any system of records containing PII developed or operated for Fiscal Service or to accomplish a Fiscal Service function for a System of Records (SOR)[1].

(b) In the event of violations of the Act, a civil action may be brought against Fiscal Service when the violation concerns the design, development, or operation of a SOR on individuals to accomplish a Fiscal Service function, and criminal penalties may be imposed upon the officers or employees of Fiscal Service when the violation concerns the operation of a SOR on individuals to accomplish an Fiscal Service function. For purposes of the Act, when the agreement is for the operation of a SOR on individuals to accomplish a Fiscal Service function, the Financial Agent is considered to be an employee of the agency.

3 Security and Privacy Awareness Training

The Financial Agent personnel who require access to Fiscal Service information or information systems will be required to review and sign Rules of Behavior, and complete security awareness training prior to being granted access. Security and Privacy training will be required on a recurring annual basis, of all Financial Agent staff performing work for Fiscal Service on a recurring annual basis, provided by Fiscal Service and/or by the Financial Agent. Access may be revoked if the annual security training is not completed. When necessary, Financial Agents will be required to sign Non-disclosure agreements.

[1] "System of Records" is defined as a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

4 Federal Regulatory Requirements and Industry Standards

- Fiscal Service Baseline Security Requirements (BLSRs)
- FIPS 140, Security Requirements for Cryptographic Modules
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
- NIST Cybersecurity Framework 2.0
- NIST Privacy Framework
- NIST SP 800-37
- NIST SP 800-53
- NIST SP 800-53A
- NIST SP 800-63-3
- NIST SP 800-137
- NIST SP 800-171
- OMB Circular A-123
- OMB Circular A-130
- Public Law 93-579, The Privacy Act of 1974
- IRS Publication 1075
- TD P 85-01 - Treasury Information Technology Security Program
- TD P 15-71 - Department of the Treasury Security Manual
- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)
- SSAE 18 or equivalent
- CISA Binding Operational Directives and Emergency Directives