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

Requirements for Statements of Qualifications and Applications to Provide Prepaid Debit Card Services for the U.S. Debit Card and Digital Pay Program

Table of Contents

I. Overview 3
II. Projected Volumes 4
III. Financial Agent Selection Process 5
A. Legal Authority 5
B. Timeline for Selection 6
C. Evaluation of Proposals 6
IV. Application Submission Process 8
A. Application Format 8
B. Deadline 9
C. How to Submit Applications 9
D. Questions 9
V. Application Package 9
I. Transmittal Letter 9
II. Part I of the Application 10
III. Part II of the application 11
1. Debit Card Features 11
2. Digital Pay Requirements 13
3. Card Stock 17
4. Account Management and Card Distribution 17
5. Card Funding 18
6. Settlement Processing/Reconciliation Integration 18
7. Activity Reports 18
8. Proposed Pricing Structure 20
9. Personnel/Infrastructure Capabilities 21

10. Customer Service – Payment Recipient 22
11. Customer Service – Federal Agency 22
12. Service Level Requirements 23
13. Security Compliance 23
14. Governance 24
15. Implementation and Transition Plan 24
16. Innovation 25
17. Educational/Public Relations Services 25
18. Media and Other Inquiries 26
19. Regulations 26
20. Garnishments 26
21. Setoff 27
22. Fraud Monitoring and Investigation 27
VI. Appendices 27
Appendix A – Payment Recipients - Transaction Types 28
Appendix B - Call Center Statistics 29
Appendix C – Program Statistics 30
Appendix D - Service Level Agreement 34
Appendix E - Attachment A for FASP 35
Appendix F - Fiscal Service Policy for Financial Agents – Data Breaches of Sensitive Information 39
Appendix G – Definitions 45

I. Overview

The Bureau of the Fiscal Service (Fiscal Service) is the bureau within the United States Department of the Treasury responsible for disbursing federal payments. A major goal of the Fiscal Service is to reduce the number of paper checks it disburses by moving check recipients to electronic payment mechanisms. As part of its All-Electronic Treasury initiative, the Fiscal Service (at that time Financial Management Service [FMS]) issued a Final Rule at 31 CFR Part 208 in December 2010 requiring that all non-tax payments be issued by Electronic Funds Transfer (EFT), with limited exceptions. The U.S. Debit Card and Digital Pay Program (USDC) provides federal agencies with the ability to deliver federal non-benefit payments (both recurring and non-recurring) through debit cards and digital payments as an alternative to checks, drafts, cash, and other non-electronic mechanisms. Fiscal Service has legal authority to provide debit card and other payment, collection, and cash management services to agencies under 31 U.S.C. §§ 321, 3321, 3322, and 3332.

The purpose of the Financial Agent Selection Process (FASP) is to select the most qualified financial agent (FA) to administer the USDC. The project deliverables shall include broad advertisement of the FASP and solicitation in an open competition FASP, a thorough analysis of all financial institution (FI) proposals, an exhaustive and intensive interview process with a limited number of FIs who are selected as finalists, and the selection of the winning FA. The high-level requirements for this FASP include existing agency funds programs and new cardholder funds programs.

Fiscal Service sponsors the USDC and specifies the card features, digital accounts, and fees. However, the FA issues the cards or digital payments and holds the legal account relationship with the payment recipients or customer agency. Once Fiscal Service disburses payments to the USDC accounts, the funds belong to either the customer agency or the payment recipients. The FA is liable for any unauthorized use of USDC that it cannot recover from payment recipients under Regulation E or the card association rule when the funds belong to the cardholder and not the customer agency. Ownership of the funds once disbursed, will depend on the requirements of the agency program the USDC is servicing. If the funds are cardholder funds, they belong to the cardholder and then once disbursed, the applicant is responsible for liabilities associated with negative balances and fraud. If the agency program requires that the funds are agency funds, then ownership of the funds resides with the agency.

In an agency funds program, the agency moves funds to a debit card that will be used by the agency employee to fulfill or carry out agency work. In addition, the agency employee is required to provide receipts and documentations to support expenditures for the government. And for the cardholder funds program, the agency makes federal payments that the agency owes to non-agency employees.

Each responding FI will be evaluated on its ability to deliver services against the selection criteria required by these programs: (a) USDC provides federal agencies with the ability to deliver Federal non-benefit payments through debit cards, as an alternative to checks, drafts, cash, and other non-electronic mechanisms; and (b) Digital Pay program that provides digital payments using email and phone number to agency payments recipients. The USDC supports 20 federal agencies with 110 programs. As of March 22, 2021, there are 148,064 active cards (non-Economic Impact Payment (EIP)), 11+ million cards in total related to EIP rounds 1 and 2 issuance that resulted in $6.4+ billion and $7.1+ billion disbursed respectively, and 4.7+ million cards issued (as of March 22) for EIP 3 associated with a disbursement of approximately $10+ billion. The Digital Pay program currently supports two federal agencies with total of four payment programs with total of $540k + of total disbursement.

While the majority of the USDC agency and cardholder funds programs require standard implementation of debit card and digital pay features and services, other agency programs require very specific and unique requirements that an FI needs to be able to address. In addition, there could be programs that need to be implemented quickly in the event of natural disasters, new legislation, or any other unforeseen circumstance, which would require FA to manage a large-scale program (i.e., stimulus payments delivered via EIP cards) to produce and distribute a significant amount of cards in short period of time while managing current agency programs.

II. Projected Volumes

Fiscal Service cannot predict the number of federal non-benefit payments to individuals or federal agencies who will be utilizing the USDC at the time of FA selection. However, historical data and recent volume trends can provide information regarding scale (see Appendix C for Program Statistics). The USDC currently serves 20 federal agencies across over 110 agency programs and it is steadily expanding.

Fiscal Service may determine that the services to be provided by the FA selected under this solicitation will be limited to services pertaining to current agency funds programs, some existing cardholder funds programs, and new USDC enrollments. However, some existing cardholder funds programs may remain with the current FA until existing issued cards expire.

Fiscal Service cannot and does not guarantee (1) the number of federal agencies who will participate in this program in the future; (2) the total dollar amount of the federal non-benefit payments; (3) the number or types of transactions that the payment recipients will complete; or (4) any other information about expected payment transactions that will occur in the future.

III. Financial Agent Selection Process

A. Legal Authority

Pursuant to its authority under 12 U.S.C. §§ 90 and 265, 31 C.F.R. §§ 202 and 208, and other federal laws, Fiscal Service is authorized to designate an FA for the purpose of disbursing federal non-benefit payments electronically through debit card. These statutory authorities and implementing regulations require that FAs be FIs that meet certain requirements. Potential applicants are thus limited to FIs that meet the requirements described in 31 C.F.R. § 202. Notwithstanding this limitation, FIs may contract with other service providers including non-FIs such as processors or financial technology companies (FinTechs) to provide the services solicited in this document. Also, Fiscal Service encourages interested FIs to consider partnering with or contracting with small FIs, or other businesses, including minority-owned or women-owned FIs and businesses, to assist in providing the required services. The application must be submitted by the FI and the FI will have the legal relationship with Fiscal Service and liability and responsibility to Fiscal Service for any services provided by its contractors.

NOTE: Applicants are selected and designated in accordance with Fiscal Service's FASP. The Federal Acquisition Regulations do not apply to the FASP.

Fiscal Service will accept applications from FIs with the demonstrated ability to issue debit cards and digital payments with the attributes described herein. Interested FIs must submit applications in accordance with the process described below. Fiscal Service will review the applications and select one or more FIs to be finalists. Finalists will be invited to participate further in Fiscal Service's selection process, which may include oral presentations and informal discussions. Fiscal Service will provide finalists with the proposed Financial Agency Agreement (FAA) that the designated FA will be required to sign. Finalists must express their willingness to sign the FAA (subject to mutually agreed-to modifications) prior to proceeding with the FASP. Fiscal Service will require the designated FA to execute a final FAA approximately four (4) weeks after the selection is made.

The FAA will be for a period of no less than five (5) years with the possible inclusion of two 2-year extension periods. We recognize that given the current size of the program, with the number of cards and the spend that flows through this payment program, the year-over-year revenues have the potential to be less than a FI requires to cover the program related expenses. We want the selected FI to know Fiscal Service is committed to payment modernization that supports Treasury's all-electronic payment initiative by moving to all-electronic payments, and that could significantly increase the flow of funds through this program.

B. Timeline for Selection

Fiscal Service's process for selecting an FA is expected to follow the timeline below (although Fiscal Service may vary the timeline as necessary or appropriate and without advance notice to FASP participants):

Date	Event
April 9, 2021	Fiscal Service issues announcement seeking applications
May 10, 2021	Application submissions due to Fiscal Service (5:00 p.m. ET)
June 11, 2021	Fiscal Service notifies finalists and non-finalists
June 11, 2021 – July 29, 2021	Fiscal Service sends sample FAA to finalists; finalists invited to make oral presentations if applicable; Fiscal Service review period
August 6, 2021	Fiscal Service designates FA and will start negotiating FAA; Fiscal Service start planning for transition (if applicable)
September 15, 2021	Selected FA signs FAA, begin transition (if applicable)

C. Evaluation of Proposals

The evaluation of proposals will be based on multiple factors and not solely pricing or costs of the services. As a threshold matter, all applications must demonstrate an ability to meet or exceed all the requirements set forth in this document and must comply with Section IV, Application Submission Process. Applications that meet these requirements will be evaluated in Phase 1 and Fiscal Service will select up to four finalists who will proceed to Phase 2. After evaluating the Phase 2 proposals, Fiscal Service will decide, in its sole discretion, which finalists to interview.

Evaluation factors for Phase 1 include the following:

- **Debit Card and Digital Pay Program Requirements.** Experience in delivering prepaid debit card and digital payment services.

- **Payment Recipients Fee Schedule.** To meet or improve existing USDC fee schedule for both debit card and digital pay service. See Appendix A: Payment Recipients - Transaction Types.

- **Cost.** The proposed cost of providing the services, including both initial start-ups, operational/on-going service, total program costs to the government over the life of the agreement, and transition (if applicable) costs.

- **Innovation.** Commitment to industry standards and innovation and incorporating innovative solutions to debit cards and digital payments services, or other advancement in electronic payments that positively impact customer service and program efficiencies.

- **Expertise of Personnel and Program Management.** Demonstrated excellence in program management, including the experience and expertise of key personnel team members.

- **IT Strategy and Development.** Expertise in electronic payment software development and managing large complex electronic payment efforts.

- **Security Compliance.** Expertise in data security and privacy controls, the protection of personally identifiable information, defense against hacking, fraud prevention in the debit card and digital payment environment, and ability to provide resiliency, redundancy, and disaster recovery (FI should include disaster recovery plan).

  See Section 13 and Appendix E - Attachment A for FASP external service security requirements and Appendix F - Fiscal Service Policy for Financial Agents – Data Breaches of Sensitive Information.

- **Customer Service and Program Administration.** Ability to communicate with customers via an interactive voice response (IVR) or similar and customer service representative (CSR) systems, email, chat, and text message, and meet requirements in Service Level Agreements (see Appendix D: Service Level Agreements) that impact the customer experience and overall responsiveness to customers.

- **Fraud Prevention, Detection, and Handling.** Ability to prevent, detect, and manage fraud without unduly disadvantaging cardholder access to funds and ability to transact on their accounts.

- **Transition Costs/Plan.** For applicants other than the incumbent, ability to transition the program in a manner that minimizes disruption to the current agency programs.

Evaluation factors for Phase 2 include the factors listed for Phase 1, and the following additional factors:

- **Payment Recipients Fee Schedule.** To meet or improve existing USDC fee schedule for both debit card and digital pay service. See Appendix A: Payment Recipients - Transaction Types.
- **Cost.** The proposed cost of providing the services, including both initial start-ups, operational/on-going service, total program costs to the government over the life of the agreement, and transition (if applicable) costs.

Selections will be made based on Fiscal Service's determination of the best interests of the government.

IV. Application Submission Process

FIs submitting applications must comply with the following requirements. Fiscal Service may, at its discretion, waive any of the requirements based on its assessment of what is in the best interest of the United States.

A. Application Format

An interested FI may submit an application in whatever format it deems appropriate, subject to the following parameters:

1. The application (excluding the transmittal letter) must be clearly divided into two sections entitled "Part I" and "Part II." Part I may not be more than five (5) pages and Part II may not be more than thirty-five (35) pages. A page is 8-1/2" x 11", single-sided, with font size no smaller than 12 point, except charts may include font size no smaller than 10 point. For Part II of the application, each section should be titled accordingly (i.e. Section 1- Debit Card Features, Section 2 – Digital Pay Requirements, etc.).
2. In addition to the 40 pages allotted to Parts I and II, the application may also contain a table of contents, pricing and costs proposal charts, and sample debit card issuance, usage, and other types of reports.
3. Nothing in the application should be marked "proprietary or confidential" however pricing or other information that the FI would not want to be released or disclosed in the event of a Freedom of Information Act (FOIA) request can be marked "program sensitive" to indicate that it is proprietary or sensitive business information.

4. The FI may not submit any sales brochures, videos or other marketing information; and
5. Responses must be written in plain English, defining each requirement in a succinct, operational manner.

B. Deadline

Applications are due May 10, 2021 by 5:00 pm ET. Fiscal Service will send a confirmation of receipt by e-mail. Fiscal Service may, in its discretion, accept applications and related materials received after the deadline.

C. How to Submit Applications

Completed transmittal letters and applications must be transmitted to the Fiscal Service email address: USDebitCardFASP2021@fiscal.treasury.gov. Applications must be in .pdf format and will be accepted via electronic mail so that the documents cannot inadvertently be corrupted or modified in the transmission and downloading process.

D. Questions

Any questions regarding the application submission process and program requirements must be submitted to Fiscal Service via e-mail, at USDebitCardFASP2021@fiscal.treasury.gov. Fiscal Service will answer all questions as soon as possible and post questions and answers on https://fiscal.treasury.gov/us-debit-card/. Unless an FI is notified in writing that the deadline for submission has been extended, the FI must submit its application by the deadline regardless of any outstanding questions it may have.

V. Application Package

The application package shall consist of the following major parts and include the FI's responses from the following requirements sections:

A. Transmittal Letter
B. Part I of the Application
C. Part II of the Application

I. Transmittal Letter

The application must contain a transmittal letter as described below:

1. The transmittal letter must be written on the FI's letterhead and signed by an official of the FI with legal authority to represent and bind the institution to the statements made in

the application (scanned signatures page or digital signatures are acceptable if the letter expressly states that Fiscal Service may rely on such signature as if it was an original);
2. The transmittal letter must include the name, title, mailing address, e-mail address, telephone number(s), and fax number of the FI's contact person to whom Fiscal Service will address all communications related to the FASP.
3. The transmittal letter must affirmatively state that the applicant (1) qualifies as an FA under 31 C.F.R. 202; (2) agrees to the selection approach described in this "Requirements for Statements of Qualifications and Applications to Provide Prepaid Debit Card Services for the U.S. Debit Card and Digital Pay Program" (3) understands that the selection process is not subject to the Federal Acquisition Regulations; (4) understands that Fiscal Service makes no guarantees that the FI will be invited to participate further in the selection process; (5) understands that Fiscal Service makes no guarantees for future volume under a debit card and digital pay program; and (6) understands that Fiscal Service may decide to select an FA to provide services for the USDC in its entirety (existing and new enrollees) or only for new enrollees.

II. Part I of the Application

Part I of the application must address the following:

1. The applicant's qualification to act as an FA for the purposes described in this document pursuant to 12 U.S.C. §§ 90, 265 and in accordance with the requirements set forth in 31 CFR § 202 and 208.
2. The identity of any partners, contractors, or affiliate organizations (collectively "partners") with which the FI proposes to provide the requested non-benefit payment services.
3. The capacity of the FI and its partners to issue prepaid debit cards and digital payments worldwide and the maximum number of debit cards it could service.
4. The ability of the FI and its partners to establish reloadable and single load electronic payments to accounts covered by Federal Deposit Insurance Corporation (FDIC) insurance and comply with any regulatory requirements that are currently enforced or any proposed requirements for these types of payments in the future.
5. The ability of the FI and its partners to establish and staff a customer service center(s) with US citizens or lawful permanent residents within the Continental United States within 90 days from the effective date of the FAA. Applications must outline the FI's experience in customer service operations including the number of call centers operated, the number of calls/transactions per month handled, customer satisfaction ratings, hours of operations, FI's interactive voice response (IVR) or similar and customer service representative (CSR) systems capabilities, and years of experience.
6. The experience of the FI and its proposed partners issuing prepaid debit cards and other types of electronic payments for recurring or non-recurring payments disbursed by a

government or private entity including a clear and concise description of projects that illustrate the capabilities of the FI and its proposed partners, as well as information about the scope and length of each project described. The description(s) should demonstrate the FI's ability to be flexible in making system, operational, and/or managerial changes to support a dynamic program, and its ability to meet the varying needs of unique agency programs while determining innovative ways to reduce checks and cash from internal business processes. Additionally, the experience of the FI and its proposed partners issuing a significant number of prepaid debit cards for recurring or non-recurring payments disbursed by a government or private entity in a short period of time while managing the current agency programs. The description should demonstrate the FI's ability to implement a large-scale program efficiently and effectively, ensuring that agency program needs are determined and addressed, while meeting short deadlines. The FI should also demonstrate experience in managing marketing, communications, and inquiries related to any and all agency programs and implementations that may be a result of a large-scale implementation. The applicant should also provide the contact information of the references for each of the major pre-paid debit card and electronic payments similar projects for governmental or private entities described above.

7. **Expertise of Personnel:** The applicant's organizational and staffing chart and biographical information of key personnel and any partners or contractors, including the following**:** names, titles, business addresses, and experience of proposed key project personnel.
8. **Program Management:** The applicant should describe how it will manage the project based on FI and its proposed partners organizational and staffing breakdown, their expertise, and project functions. The experience of the FI and its proposed partners while managing both small-scale and large-scale agency programs, to manage its processors and/or contractors. For instance, how FI will manage expirations of debit cards nearing the end of FAA.

III. Part II of the application

Part II of the application must address, in order, all the following:

1. Debit Card Features

A description of debit card features for the product(s) offered to meet the stated objectives, including whether the following features will be available:

a. Applicant must be able to provide the following:
   i. Branded and unbranded cards with the capability to provide prepaid debit cards that can be used worldwide;
   ii. ATM only cards;

iii. Instant issued cards;
    1. Ability to provide immediate funds loading and funds availability
    2. Define instant issue funding process
iv. Capability for personal identification number (PIN)-based or signature-based transactions at ATMs or POS devices;
v. Cardholder ability to withdraw funds at a bank or credit union branch or other ability to withdraw some or all funds off the card;
vi. Single Deposit Cards – Branded or unbranded, may not be reloaded and is non-personalized. Funds deposited may be agency-owned or cardholder owned;
vii. Multiple Deposit Cards – Branded, reloaded, personalized or non-personalized. Funds deposited may be agency-owned or cardholder owned;
viii. Cardholder's name embossed on the card, other agencies may dictate specific information that needs to be printed on cards;
ix. Other information required to be printed at the back of the card may differ by agency programs (i.e., agency customer support number and website).

b. Provide a step-by-step description of the process for establishing an account record. Include a start to finish timeframe, quality assurance and controls, and reporting features. The account record is the infrastructure necessary to support a federal agency program or business line. A federal agency program or business may require one or both of the following:
    i. Individually owned accounts in the name of the cardholder;
    ii. Government agency owned funds – agency owned accounts in either the name of the cardholder, or name specified by agency.
c. Card Network design:
    i. The Applicant must provide a generic card design and ability to provide multiple custom card design options as requested by customer agencies.
d. Explain management of agency program(s), for example the tracking of overall card issuance and balances, or number of loads;
e. Describe the process for assigning sub-account or parent-child accounts routines for each federal agency program or account;
f. Ability for cardholder to add cardholder-owned funds to a separate personal debit purse to augment public transit benefits, as needed, and if not, the Applicant must provide an alternative solution for allowing cardholders to add separate funds, if possible;
g. Ability to add or remove card parameters for Merchant Category Codes (MCC) and merchant identification numbers;
h. Ability to load balances at monthly or regular intervals or at the request of the federal agency;
i. How the Applicant will handle "inactive" cards, including how the Applicant defines "inactivity;"

j. FDIC insurance for cardholder funds;
k. Regulation E protections for cardholders (describe protections that will be available);
l. A unique routing number(s) designated specifically to card accounts under the program; unique BIN(s) designed specifically for the program;
m. Card-related security features:
    i. Europay Mastercard and Visa (EMV) chip with PIN and signature capabilities for all cards.
n. Require flexibility to determine card expiration;
o. Ability to load large (i.e., $100,000) dollars to cards if agency requires; and
p. Ability to provide the capability for near field communication (NFC).

2. Digital Pay Requirements

The Applicant's capability to provide Digital Pay services as additional payment delivery mechanism that includes the general requirements for the following accounts:

Virtual Account Services:

a. Deliver digital payments using email and phone number;
b. Cancel and re-initiate payments;
c. Flexibility with the Virtual Account set-up, capability to use account in covert manner (i.e., no link between digital payment recipients and account created in a program);
d. Deliver electronic payments to a recipient's existing bank account through ACH credit or direct to debit;
e. Deliver payments to a recipient's "Virtual Account," for example, a PayPal account or Apple Pay wallet or similar product, or to transmit funds to an eligible account using the payment recipient's debit card number;
f. Provide plastic card upon Virtual Account owner request. Virtual Accounts for which plastic debit cards are provided will be governed by definitions identified in Appendix G. For account owners who request physical cards, the FA shall offer agencies the option of using one of two standard card stocks;
g. Capability to establish agency or recipient's Virtual Accounts at the direction of Fiscal Service;
h. Capability to establish all Virtual Accounts with an Issuer Identification Number (IIN) unique to the USDC;
i. Provide all necessary settlement processing for account transactions, including access to ATM networks, Point-of-Sale (POS) networks, and third-party wallets, and ensure proper reconciliation requirements are met;
j. Ensure that all Virtual Accounts are capable of receiving federal payments but will not allow an account owner to load personal funds to the account;

k. Provide a Virtual Account holder with the ability to view account balance, review account transactions, make online payments, and transfer money from the account to another account via an interactive voice response (IVR) system, mobile interface, and secure website; and
l. Subject to the approval of Fiscal Service, provide Virtual Account instructional information and disclosures to Virtual Account holders in accordance with applicable laws and regulations. All materials will be in easy to understand English. Most programs will use generic USDC instructions and disclosures; however, some programs may require modified carriers to include Agency logos, product names, or Agency POCs.

Agency Virtual Accounts:

a. Applicant's capability to provide a means for managing agency Virtual Accounts, including activating and deactivating accounts, loading and reloading accounts, assigning Personal Identification Numbers (PINs), reissuing virtual account and supporting balance and transaction inquiries applicable to each account type;
b. Applicant's capability to provide agencies with the option to have cards embossed with an individual name or a generic phrase selected by the agency;
c. Applicant's capability to provide agencies with the ability to restrict the capabilities (i.e., deposit money to virtual account) offered to the Virtual Account owner;
d. Applicant's capability to provide the following agency reporting requirements:

    i. Agency-level reporting available via its web-based system and available reports from the FA's web-based client platform. The FA shall maintain details on data elements and report format in its web-based client manual;

    ii. Transaction records available to agencies on the following business day;

    iii. Reports available in .csv file format, which agencies may save locally and/or import into other applications, such as Microsoft® Access or Excel;

    iv. Available reports from the FA's web-based client all "standard" reports for applicable programs as defined below. Title of the reports are for informational purposes only, Fiscal Service will accept different variations.

        1. Enrollment Status Report: Provides users with enrollment status information.

        2. Customer Profile Report: Provides a report that will identify the number of accounts per profile and list all the Virtual Account holders for a specific agency.

3. Pending Enrollment Confirmation Report: Shows all enrollments where the required hardcopy documentation has not been received within a defined period of time.

4. Batch File Processing Report: Provides the file status of the batch file received by the FA.

5. Adjustment Summary Report: Shows summary information for all funding adjustments performed within the profile for a selected date range.

6. Adjustment Detail Report: Shows the detail of each adjustment transaction within a selected profile for a selected date range.

7. Daily Transaction Report: Shows details of transaction (i.e., MCC codes) performed within a selected date range.

8. Virtual Account holder Status Activity Report: Shows account status updates (as of end of day) for a selected date range

9. Inactivity Report: Provides a list of accounts shown as "inactive" for a selected date range.

10. Instant Card On-Line Activity Report: Shows summary and detail information of all instant card load and reload transactions, if applicable.

11. Funding Summary Report: Shows the summary information for successful funding activities.

12. Funding Detail Report: Lists all Virtual Accounts and the amount that was funded into the account.

13. Activation Summary Report: Shows the number of Virtual Account activation status changes.

14. Virtual Account Activation Status Detail Report: Provides detail information on account activation status changes.

15. Client Transaction Summary Report: Shows summary level account holder account usage for a client account containing only Agency Funds.

16. Account holder Transaction Detail Report: Shows detail level account holder usage for a client account containing only Agency Funds.

17. Account Closure Report: Provides details on accounts that are ready for closure and the remaining balance amounts that are refundable.

18. Card Issuance and Replacement Report: Identifies all Virtual Account holders that requested and received a plastic card, including any replacement cards.

Consumer Virtual Accounts:

a. Capability to comply with the following regulations to:
   i. Hold the funds in accordance with the Federal Deposit Insurance Corporation's pass-through insurance requirements at 12 CFR 330.5, such that each account holder's funds are insured to the maximum extent permitted by law;
   ii. Provide account holders with the consumer protections that apply to a payroll card account under Regulation E (12 CFR Part 1005) unless and until the Consumer Financial Protection Bureau's amendments to Regulation E to provide consumer protections to prepaid account holders take effect;
   iii. Comply with the Gramm-Leach-Bliley Act, the Right to Financial Privacy Act and other applicable laws related to the protection of the account holder's privacy; and
   iv. Comply with the applicable provisions of Regulation II (12 CFR Part 235, Debit Card Interchange Fees and Routing).

b. Consumer Virtual Accounts will not accrue interest to the account holder's or the government's benefit;
c. Provide the ability to load identified accounts with a designated amount on a specific date as indicated by the agency that does not align with the FA monthly expiration cycle. The FA shall provide the ability for remaining funds from the previous balance to be reported and returned to Agency;
d. Provide the capability to integrate into an agency's accounting system for real-time processing utilizing an API which results in an online/real-time issuance and funding capability, if agency opts to use Digital Pay services; and
e. Provide the capability to transfer funds from a Virtual Account to a third party who provides the Virtual Account holder a name and email address. The FA will send a notification to the third party that the third party may accept funds via a Virtual Account such as PayPal account or Apple Pay wallet or similar product, ACH, or Direct to Debit. Transfer capabilities shall be available online via browser and via mobile app on Apple and Android operating systems.

3. Card Stock

A description of how the Applicant will obtain and provide necessary card stock, including how the Applicant will maintain sufficient quantities of card stock, issue cards in advance of enrollment and other necessary materials for program operations. The Applicant should also describe how it will obtain the large number of cards in a short period of time for large-scale or other programs and how many cards can be processed daily, weekly, and monthly.

4. Account Management and Card Distribution

A description of the proposed process for account enrollment and management, issuance of cards, and management of issued cards. The description should address the following:

a. Applicant will only accept card set up information from a federal agency. Generally, an agency will be responsible for enrolling Agency Virtual Accounts, although the FA may be responsible for enrolling accounts as determined by agency requirements.
b. Ability to provide an enrolling federal agency with routing and account information, in advance, for assignment to enrolled cardholders.
c. Describe Applicant procedures for when a request is made to close an account.
d. How the Applicant will define and handle "inactive" cards, for example, card where there have been no deposits and/or withdrawals for a period of time.
e. Distribution method requires:

    i. Instant issue with funds loaded and available instantly, other agencies require to fund cards on agency site
    ii. Bulk shipment of cards to single location
    iii. Individual card mailed to individual location or multiple mailing to a single address

f. Applicant must provide an inventory management process that can track card stock by location and ensure that federal agencies receive cards timely and accurately.
g. How renewal cards will be delivered to cardholders.
h. Procedures for mailing cards to cardholders.
i. General description of cardholder materials to be provided to cardholders with each debit card (subject to government approval), including materials that explain to cardholders how to activate and use the card.
j. Ability of FI for bulk activation and not to require PII for activation for other agency programs.
k. Cardholder activation by cardholder selected PIN and deactivation procedures.

l. Describe process for assigning PINs; ability to provide for the agency to issue or determine the PIN; send card with PIN on a pull off tab.
m. Procedures and timeframes for re-issuing lost/stolen/destroyed/expired cards; closure of account when expired; automated re-issuance 30 day prior to expiration if card has been used within 90 days of expiration.
n. For agency funds program, agency may require ability to claw back unused funds promptly.
o. For agency funds program, ability to return all unspent funds to agency (i.e., claw back funds).
p. For agency funds program, ability to return all funds to agency for inactivated cards;
q. Ability to provide an agency capability to print (embossing) and personalize cards and image on agency site via interface with DataCard Model SD260 printer and/or other agency required printers.
r. Ability to provide agency card accounts in numerical sequence.
s. Ability to provide agency with the ability to manage agency funds program accounts directly that includes searching activity or transaction data, managing card balances, and adding additional funds multiple times a day.
t. Ability to provide agency historical data of previously expired and deleted accounts.
u. Ability to describe process in monitoring and managing card issuance and card expirations and how FI oversees this process in the event of an expiration of the FAA.

5. Card Funding

A description of the Applicant's proposed card funding (load and reload) procedures via the Automated Clearing House (ACH) network.

6. Settlement Processing/Reconciliation Integration

A general description of how the Applicant's debit card and digital payment settlement processing works, including a description of the Applicant's daily and other reconciliation procedures. Applicant's ability to use settlement account via Federal Reserve Bank's ACH (FedACH)/Fedwire or utilize Fiscal Service's Automated Standard Application for Payments (ASAP) system to fund the settlement account and accept returned funds from the settlement account. Alternative settlement account funding and return mechanisms may be used by agreement of the parties. Applicant's ability to manage the settlement processes with the integration of other Fiscal Service systems such as the Treasury Offset Program (TOP) or the Secure Payment System (SPS) certification, and with considerations of any agency process, as applicable.

7. Activity Reports

A description of how and when reports are distributed and can be accessed through FI's web-based client application, whether the report information can be broken down by payment types, federal agency, agency program or business line, as well as be provided in a specific format as requested. The Applicant must provide agency capability to access reports securely and provide a description and samples of the types of reports that will be made accessible to Fiscal Service describing call center and account activity, including reports related to:

a. Lost/stolen cards;
b. False Acceptance Rate report: rate at which an unauthorized individual is accepted by the system as a valid user;
c. False Rejection Rate report: rate at which an authorized individual is rejected by the system as an invalid user;
d. Authorized user attempting to use card at non-authorized terminals;
e. Invoicing support for all fund draws from the customer agencies' accounts, i.e., a funding detail report listing payment recipient accounts and the amount that each was funded during the reporting period;
f. Detailed transmittal reports for each federal agency program/account profile;
g. An aging report of inactivated cards.
    i. Inactivity Report that details payment recipient accounts listed as "inactive" over a select date range.
    ii. Suspended Card Report that details payment recipient accounts listed as "suspended" over a select date range.
    iii. Canceled/Closed Cards Report that details payment recipient accounts listed as "canceled/closed" over a select date rage.
    iv. Cards activated but not used report
h. Change report: For any change to enrollment or status.
    i. Payment Recipient Status Activity Report – Provides details of end of day card status updates over a selected date range, inclusive of lost, stolen, and damaged status types.
    ii. Enrollment Status Report – Provides users with enrollment status information.
i. Account Status Report: Change in card account status by federal agency and agency program or business line;
j. Enrollment and customer service call center activity;
k. Aggregate funding activity;
l. Aggregate average daily balances;
m. Aggregate transaction activity;
n. Authorized limit vs. actual use by cardholder;
o. Unused portion of cardholder's benefit;
p. Specific federal agency reporting;
q. Cardholder Transaction Detail Report – Provides detail level cardholder card usage for a client account;

r. Monthly account statements that may include the following requirements:
    i. Statement period consistency (i.e., Jan 1 to Jan 31)
    ii. Format includes but not limited to bank letterhead, by a set date (i.e. by 5 business days follow month period's ending), beginning balance, ending balance, all accounts debits/credits, pdf standard format;
    iii. Capability to provide hierarchy (parent-child) on funding accounts (i.e., parent account redistributes funds from one child account to another);
    iv. Capability to access monthly account statement electronically and securely.
s. Customizable or ad hoc reports in specified format or ability to choose different parameters as requested;
t. Regular program management reports to Fiscal Service on quarterly and monthly basis with content and in a format to be agreed upon by the parties or FI capability to provide access to Fiscal Service Program Manager to report. Such reports shall contain Digital Pay program information, including information about account activity by product, transaction statistics, revenue fees by profile, program tracking information about current and prospective program agencies; and
u. Ability to respond to data requests by Fiscal Service in a short time (i.e., 24 hours or less). Due to the nature of USDC, the program is subject to a high-level of scrutiny (i.e., congressional/FOIA request or audit) and as a result, the expectation is that the selected FA will be responsive to ad-hoc data requests.

8. Proposed Pricing Structure

a. Pricing Proposal
    i. **Payment Recipients Fee Schedule:** Applicants must submit bids that are based on current USDC transaction types (see Appendix A: Payment Recipients - Transaction Types). Competitive Applicants should reduce or eliminate one or more transaction type fees. In direct support of this, Fiscal Service expects equal or greater coverage of surcharge free Network ATMs with this proposal.
    ii. **Compensation:** The proposed compensation for providing the services should include operational/on-going service, total program costs to the government over the life of the agreement, and initial start-up/transition (if applicable) costs. Pricing proposals should address financial compensation for operational costs based on the assumption that the Applicant would provide services for all USDC agency programs (existing and new). Program statistics regarding stimulus payments are included only for future scale purposes of the program, however existing economic impact payment cards will not be part of the transition if a new FA is selected. The incumbent should assume that the services to be provided cover all USDC agency programs. Applicants should state how much, if any, compensation from Fiscal Service is required and explain how that amount is calculated. The Applicant may use any

methodology for calculating required compensation – for example: per cardholder; one-time versus periodic; variable based on card usage; or other assumptions. The Applicant should provide a transparent and clear explanation of the rationale for any operational cost compensation proposal. Similarly, if it is determined that zero compensation is needed, the Applicant should also provide a transparent and clear explanation of the rationale supporting that decision. Any initial start-up/transition-related costs must be identified and defined including any build out or infrastructure costs.

b. **No Credit Check; Cardholder Retention:** Any pricing structure should assume that potential payment recipients may not be subject to any credit screening requirements and that cardholders, once enrolled, will not be terminated on the basis of dispute claims or suspected card misuse other than in exceptional circumstances and only with the notification of the government.

9. Personnel/Infrastructure Capabilities

A description of the personnel and infrastructure capabilities of the Applicant to provide the required debit card and digital payment services, including the security and privacy protection features. The Applicant should include a description of customer outreach related activities and how an expanding business would be managed. The Applicant should also provide a description of how it could manage a large-scale program that would need to be implemented quickly while minimizing impact to existing customers.

The Applicant must provide information technology service capability (i.e., web-based client platform) to allow Fiscal Service and/or federal agencies to manage all aspects of all debit card and digital payments service programs related to the following:

a. Read access as required to monitor and verify participant status and usage;
b. Generate reports as required (i.e. agency and program);
c. Generate reports with date range flexibility;
d. Change cardholder status that is more immediate than next- day batch update; ability to make adjustment promptly by agency such as when there is card and or funding failure and ability to defund card and reissue a new card instantly in an agency site;
e. Access should be role-based to support multiple federal agency contacts with differing access needs;
f. The Applicant's online system must be customizable to allow for federal agency specific field names, menus, and reports; to address different agency requirements such as change to account profile, employer identification, agency point of contacts changes, and other data fields requirements;

g. Ability to order cards for new enrollments and renewals electronically;
h. Ability to access data up to a minimum of three years old;
i. Ability to view transaction level data including any fees, (i.e. ATM fees);
j. Ability to integrate into an agency's system for card issuance and funding capability; and
k. An option for an agency to access FI's information technology service via mobile phone that will allow debit card and digital payments services management functions.

10. Customer Service – Payment Recipient

There is a particular need for customer service to be available at the time of funding to a USDC payment account. A description of the Applicant's proposed payment recipient's customer services, including:

a. How a payment recipient may obtain services related to lost/stolen/defective cards, unauthorized transactions, account balance and transaction (paper statements are optional and available by request), card usage questions, online payments, transfer money from the account to another account via an interactive voice response (IVR) or customer service representative (CSR) systems, mobile interface or application, secure website, text/email, or other innovative methods for communicating with payment recipients;
b. The Applicant must make customer service available 24/7/365;
c. Availability of ATM network nationwide, including surcharge-free network and/or other ways cardholders may obtain cash or use ATMs surcharge-free, and how the availability of a surcharge-free network and/or surcharge refunds to cardholders impacts the Applicant's proposed pricing structure;
d. Access to customer service and new technologies to handle and process customer service needs by payment recipients with disabilities, and availability of all materials and customer support services in languages other than English such as Spanish;
e. How the applicant will respond to payment recipients disputes and agency claims of incorrect payments in compliance with appropriate ATM, Card Network association, and network operating rules applicable to each card product;
f. Training and competency requirements for customer service personnel;
g. Quality control procedures the Applicant uses to monitor and confirm that customer service requirements are being met;
h. Dedicated toll-free number for government support in conformance with the Americans with Disabilities Act; and
i. Customer service center must meet or exceed established SLAs (see Appendix D: Service Level Agreements).

11. Customer Service – Federal Agency

A description of the customer service and support that will be available to Fiscal Service and federal agencies whose programs are participating in the USDC, including project management controls, assistance with the Applicant's system (if necessary), report inquiries, and a description of the type of support the applicant would be able to provide to a federal agency investigating a cardholder's current card status (for example, account balance information).

Provide communication support for debit card program to Fiscal Service and federal agencies participating in program through meetings, literature and other means, and provide information to be shared at meetings in advance. For agency programs, customer service options may vary based on the program.

Fiscal Service expects excellent customer service that will support USDC program agencies. Applicant's on-site point of contact in Washington, DC area that can meet regularly with Fiscal Service and any agency located in the area.

12. Service Level Requirements

A description of how the Applicant plans to meet performance measures related to customer service and deposit processing and documentation demonstrating experience in other card programs where performance measures were met or exceeded. See Appendix D: Service Level Agreements for specific requirements.

13. Security Compliance

The Applicant's ability to comply with all applicable security requirements of Treasury directives and Fiscal Service policies:

a. Treasury directives require that employees, who are working on this project, including call center employees, must be US citizens or lawful permanent residents.
b. The FA is providing a banking service to Fiscal Service and agencies. To the extent necessary, the FA shall assist and work with Fiscal Service to comply with security requirements of external service as part of continuous monitoring. Appendix E - Attachment A for FASP for external service security requirements and Appendix F - Fiscal Service Policy for FAs – Data Breaches of Sensitive Information. The FA will not be operating an information system on behalf of Fiscal Service.
c. The FA shall provide Fiscal Service a yearly Statement on Standards for Attestation Engagements no. 18 (SSAE 18) audit report in electronic format. Fiscal Service will treat the SSAE 18 as confidential. If the SSAE 18 or any related documentation is the subject of a Freedom of Information Act (FOIA) request, Fiscal Service will give the FA the opportunity to indicate what information constitutes trade secrets or commercial or

financial information that is confidential, the release of which could harm the FA. Fiscal Service will assert the exemption under FOIA that allows for protection of that information, as well as any other FOIA exemption that might apply and promptly notify and cooperate with FA so that FA may contest the disclosure of the proprietary information.

d. The FA shall participate in government audits and provide information/data as necessary to fulfill the nature of the audit, and as authorized and/or not prohibited by law.
e. A general description of the Applicant's emergency and disaster recovery and contingency plans in the event of primary systems failure or other similar event, including call center locations, to be transferred to an alternate system and/or facility.

14. Governance

The Applicant will play a key role in all federal governance structures and processes, assisting in the drafting and maintenance of all artifacts--particularly a detailed alternatives analysis-- data calls and reports required by Fiscal Service, the Office of Management and Budget (OMB) and/or other federal entities. The Applicant will be required to comply with Fiscal Service security, testing, change control, enterprise architecture, data retention, data protection, governance, record management, and other requirements.

15. Implementation and Transition Plan

Each USDC federal agency customer may have several different agency programs utilizing the USDC in different ways. Transitioning each type of program and each agency may require a unique approach in order to minimize impact to customer agencies and cardholders. Applicants other than the incumbent must provide a high level project implementation and transition plan for USDC current and potential customers, including estimated implementation and transition timelines, a description of how the applicant would manage the transition and implementation of the program and maintenance of documentation to support the project must be included. The plan should describe how the transition would work and how the Applicant would manage the transition and must include a list of key transition team personnel and their roles and responsibilities. Plans must also include an initial milestone schedule to be completed within six months of executing the FAA, and not to exceed a year. The Applicant should explain any potential risks and identified level of risks associated with each stage of the transition.

Applicant can refer to Appendix C that describes the overall summary of the current USDC (i.e., average card volumes) and other potentially new large-scale program (i.e., stimulus payment) that may be implemented expeditiously.

Some of the requirements identified may be unique to the basic debit card and digital pay services, so it is important for the FI to specifically identify in the plan its ability to implement

the USDC program shortly after signing the FAA versus any requirements from this solicitation that the FI will still need to develop solutions for during the transition including the timeline on how particular requirements can be developed, tested, and implemented for an agency. For example, an agency requires the ability to manage its own issuance of cards to its cardholders and in some instances some agencies may require bulk activation that may not require PII, and distribution of cards to one specific location. Additionally, an agency may have a requirement to integrate with a specific printer so that the agency can emboss specific information and a cardholder image to the card. In another instance, an agency may require the use of debit card or digital payments to support sensitive government operations.

Applicants other than the incumbent must include in their pricing proposal any compensation required from the government associated with the Applicant's role in transitioning existing USDC accounts.

16. Innovation

Applicants should describe their experience in innovation and provide specific examples either in connection with debit card and digital payments services or other advancements in payment industry standards and/or with the use of mobile applications. For example, capability to issue payment through blockchain or worldwide money transfer application.

Applicants should describe their capability regarding data analytics that can provide USDC agency programs and Fiscal Service with data information for analysis in response to all reporting requirements or any data call requests (i.e., congressional inquiries, audits, FOIA or any government reports and requests).

17. Educational/Public Relations Services

The Applicant must implement an education plan designed to increase customer awareness of the features and benefits of the USDC. The Applicant should provide a description of the type of education and public relations the Applicant could support as part of their plan (e.g., web based training, mobile application, card carriers, brochures, customer surveys, social media, educational videos), and any applicable costs associated with such services. Education related material should focus on how payment recipients can access balance and transactional information through differing mechanisms of their choosing. The FA is prohibited from using any payment recipient's information for marketing purposes.

The Applicant must demonstrate its ability to provide training to agencies on how to use the FI's information technology system or any web-based client platform. In addition, the Applicant must demonstrate its ability to support agency customers during program on-boarding or

implementation, educate agency on overall USDC, how USDC will be set up for each agency specific implementation, and the setup of interface.

The Applicant must be a partner to Fiscal Service in providing overviews and other customer agency relations management work and assistance. For example, the FA is expected to be a partner who can support the Fiscal Service Program Manager in assisting and working with customer agencies in answering questions related to USDC and the FA's debit card and digital pay services.

18. Media and Other Inquiries

A description of the Applicant's capacity to handle media and other high-profile inquiries regarding the USDC including a description of the resources available to handle such inquiries.

19. Regulations

The Applicant will be required to adhere to the following legal requirements and regulations:

a. Newly issued and replacement cards must be equipped with EMV chip/pin technology pursuant to Executive Order 13681 – Improving the Security of Consumer Financial Transactions (October 17, 2014);
b. Identity authentication ("customer identification procedures" or "CIP") procedures and compliance with the PATRIOT Act and applicable Office of Foreign Asset Control (OFAC) and Treasury regulations;
c. If not already described, a description of the Applicant's security and privacy protection procedures, including how the Applicant proposes to comply with Gramm-Leach-Bliley Act, the Right to Financial Privacy Act, and other applicable laws;
d. FDIC insurance for cardholder funds;
e. The USDC is not exempt from the Dodd-Frank Wall Street Reform and Consumer Protection Act, "Regulation II, Debit Card Interchange Fees and Routing;"
f. Cardholders must be provided all of the consumer protections that apply to a payroll card account under Regulation E unless and until the Consumer Financial Protection Bureau amends Regulation E to provide consumer protections to prepaid card holders;
g. Must have the ability to comply with any regulatory requirements that are currently enforced or any proposed requirements for prepaid cards in the future. Applicant must describe protections that will be available;

20. Garnishments

Applicants must comply with 31 CFR Part 212.

21. Setoff

A description of how the Applicant's policies with respect to the FI's right to setoff for payment of cardholder fees, overdrafts, or other amounts as agreed to owed by the cardholder to the applicant would apply to the proposed debit card product. Setoffs for amounts owed by the cardholder to the Applicant for activity unrelated to the debit card product are prohibited.

22. Fraud Monitoring and Investigation

A detailed description of how the Applicant will prevent, detect, and handle fraud, including how the Applicant will monitor account activity for fraud; how the Applicant will respond to card accounts that have been compromised and/or erroneous enrollments; fraud mitigation tools currently employed by the Applicant, how cards are terminated; and how incidents are investigated when the Applicant believes fraud has occurred in connection with an account. Applicants must also include general information regarding incidents of fraud with respect to its payment programs and how those incidents are handled. For Agency Virtual Accounts, the Applicant's ability to assist agencies in setting up processes for protecting against fraud or misuse of the Digital Pay program, which includes providing agencies guidance on appropriate parties to have access to the FA's web-service client to be limited to government officials/contractors with pecuniary and/or fiduciary liability.

VI. Appendices

Appendix A – Payment Recipients - Transaction Types

The transaction types applicable to both Virtual Cards (Digital Pay) and physical debit cards are marked with an asterisk. Transaction types that are not marked with an asterisk are applicable only to physical debit cards.

Table A: Transaction Type

Transaction Type
Inactivity fee* (3 consecutive months of no activity)
Check (use, order, or stop payment; cash at participating check-cashing locations)
Signature Point-of-Sale Transactions (for purchases, declines and returns) | US and Non-US
PIN Point-of-Sale Transactions - with or without Cash Back (for purchases and declines) | US and Non-US
PIN Point-of-Sale Transactions - with or without Cash Back (for returns) | US and Non- US
ATM withdrawals | US In-Network ATMs
ATM withdrawals | US Out-of-Network ATMs (First Free per deposit)
ATM withdrawals | Non-US ATMs
ATM inquiries | US and Non-US
Declined Point-of-Sale (POS) Transaction
Bank Teller Over-the-Counter Cash Withdrawal (at any bank that displays the logo shown on your card)
Third-party wallet tokenization (load, transfer, or ACH) *
Transfer Funds to a Bank Account via ACH transfer*
Monthly paper statement by mail*
Periodic monthly paper statement expedited mail*
Balance inquiries and alerts via mobile app, automated phone system, Customer Service, Online Access, or Notifications (push, email or text) *
Customer Service 24/7*
Disbursement or funds transfer via Direct to Debit*
Replacement Card with Standard Delivery
Replacement Card with Expedited Delivery

*Inactivity Fees on agency programs NTE three consecutive charges.

Appendix B - Call Center Statistics

Call Center Statistics: See **Charts A** through **D**

Chart A: Call Center Volume – USDC Programs

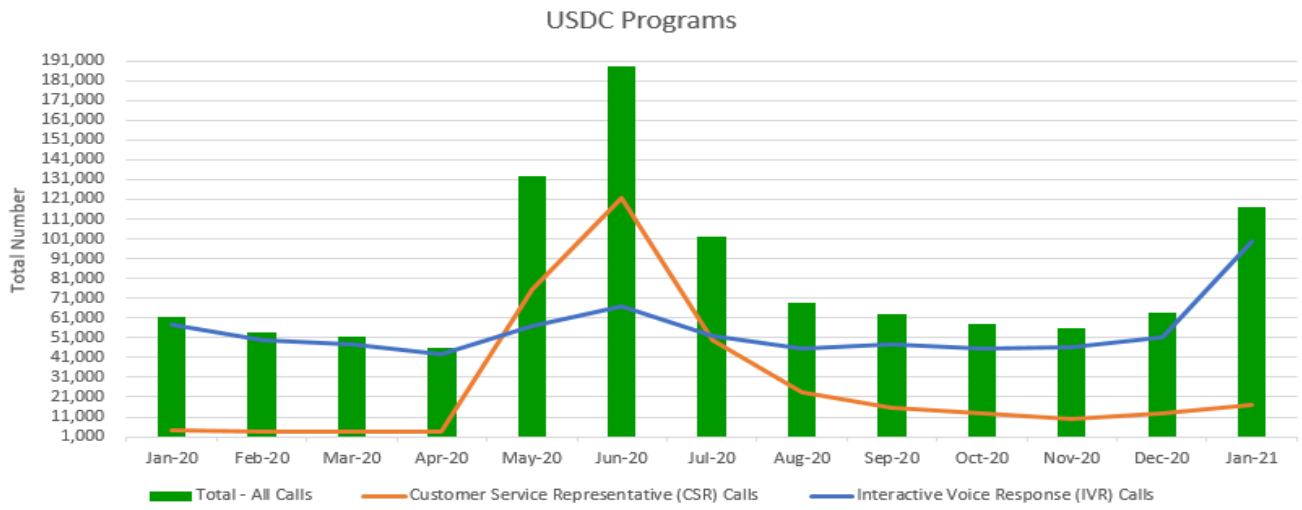


Chart B: Call Center Volume – Large-scale program

Note: The chart below represents a large-scale program (i.e., stimulus payments) scenario that could increase call center volume.
The summary data below reflects all rounds of stimulus payments as of March 31, 2021.

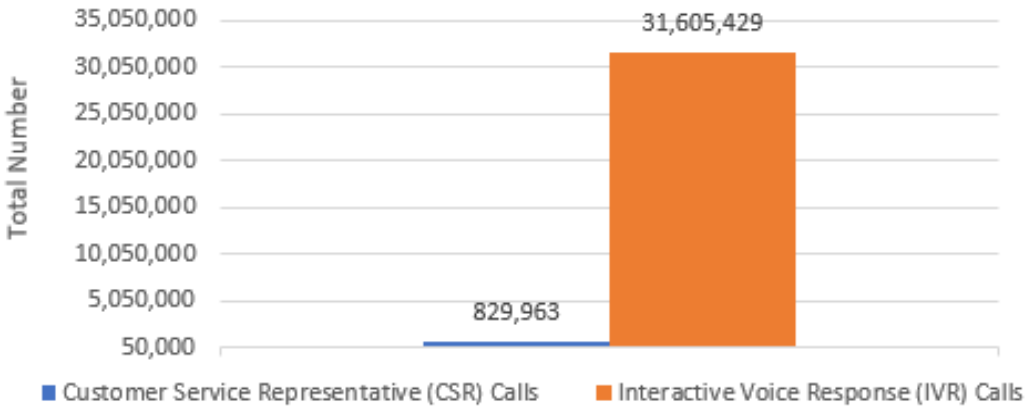


Chart C: Top Reasons of Calls Transferred to CSR – USDC Programs

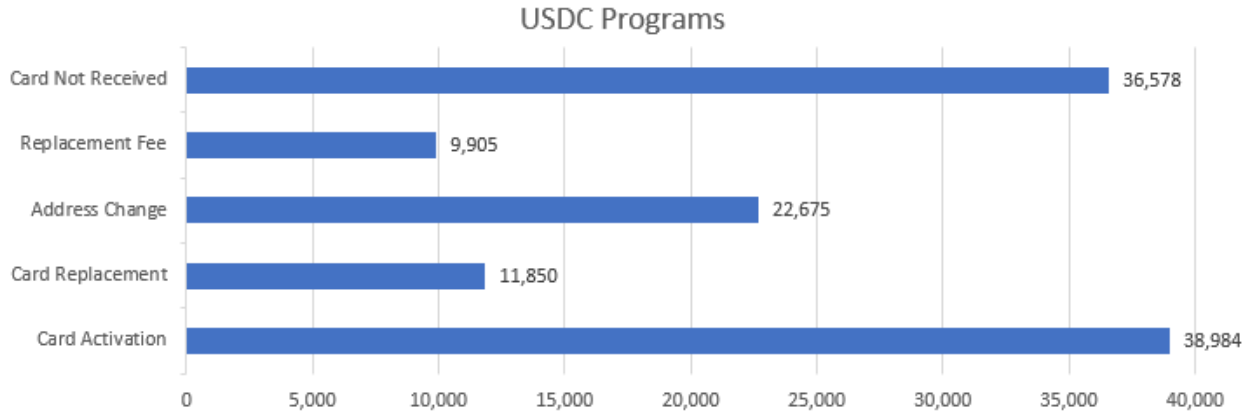
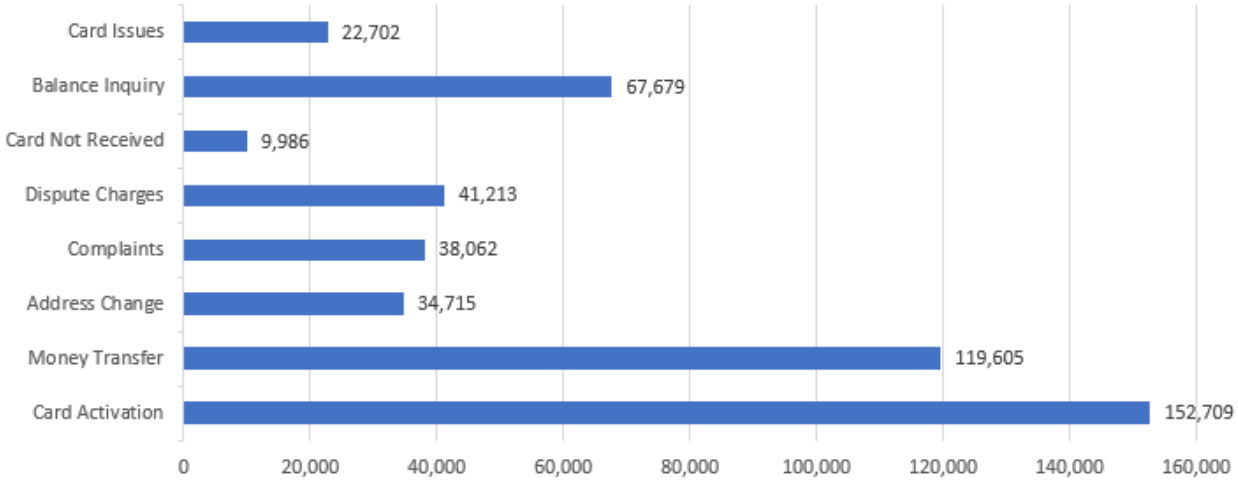


Chart D: Top Reasons of Calls Transferred to CSR – Large-scale program

Note: The chart below represents a large-scale program (i.e., stimulus payments) scenario that identify the Top Reasons of calls transferred to CSR.
The summary data below reflects all rounds of stimulus payments as of March 31, 2021.



Appendix C – Program Statistics

Program Statistics: See **Charts E** through **J**

Chart E: Cardholder Balances – USDC Programs

This chart represents the cumulative monthly cardholder dollars loaded and the average monthly balance for active cards for the reporting period.

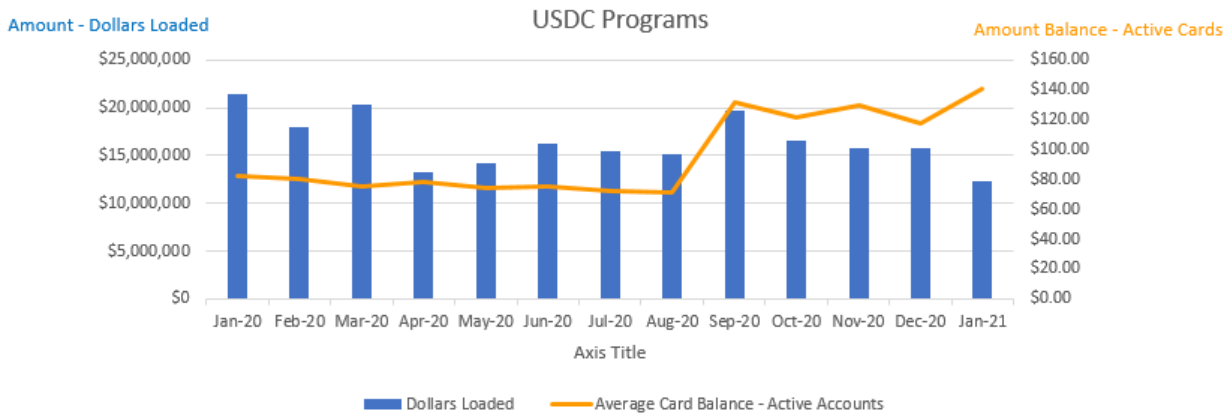


Chart F: Cardholder Balances – Large-scale program

Note: As of March 23, 2021, the chart below represents a large-scale program (i.e., stimulus payments) scenario that could impact FI's quarterly statement reporting. For round 3 of stimulus payments, the average card balance on active accounts data is not yet available.

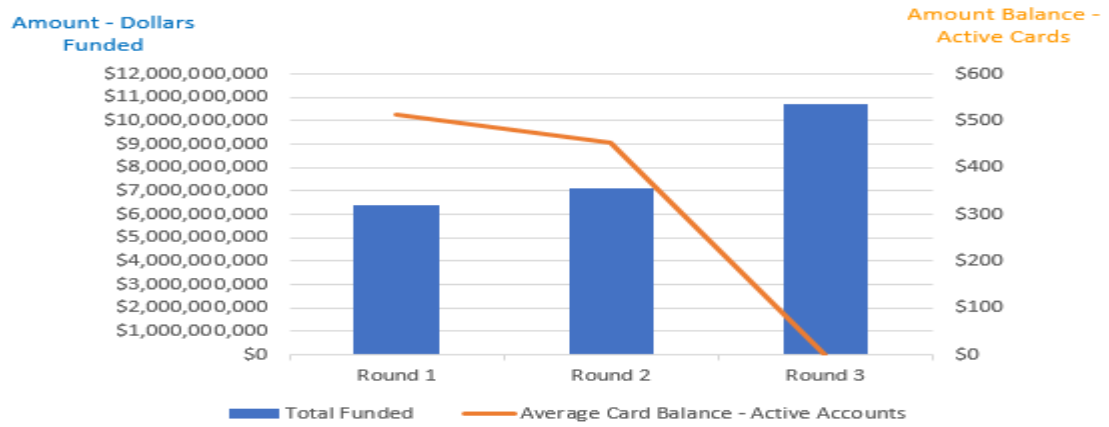


Chart G: Account Volume – USDC Programs

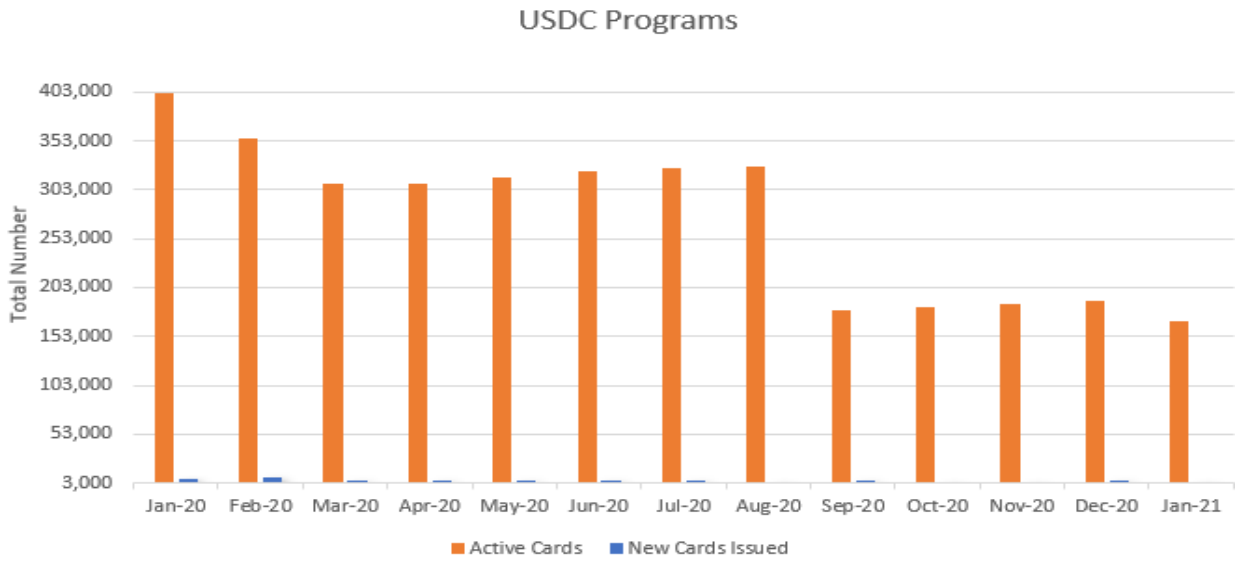


Chart H: Account Volume – Large-scale program

Note: The chart below represents a large-scale program (i.e., stimulus payments) scenario of the total cards issued and activations. For round 3 of stimulus payments below, the total of cards issued* are cards produced and mailed, and the total activations are data as of March 31, 2021.

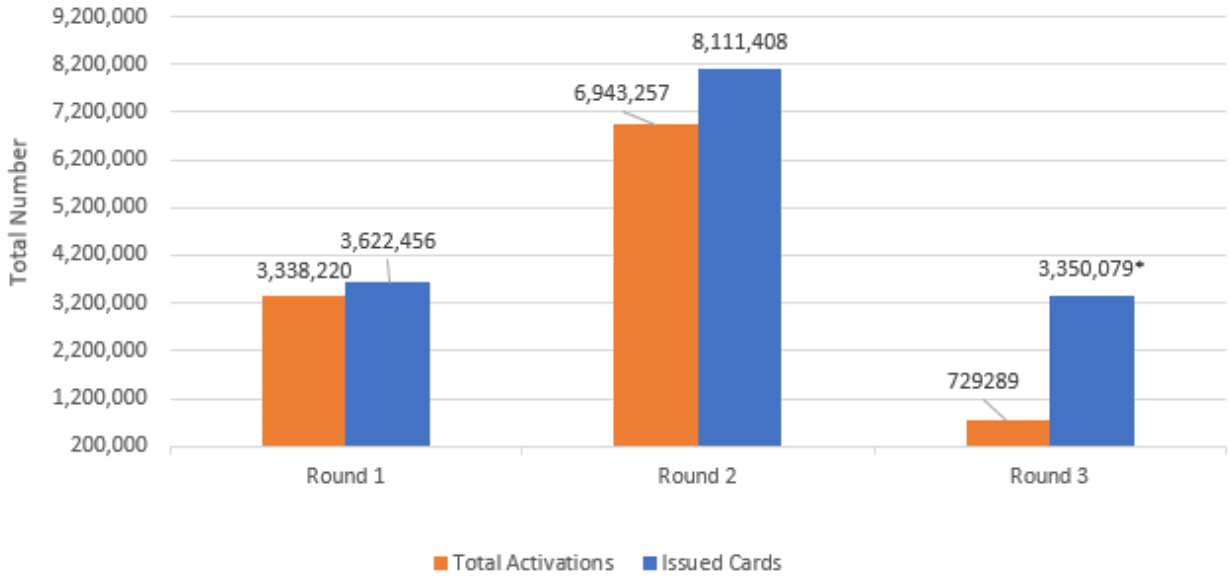


Chart I: Spend Rate – USDC Programs

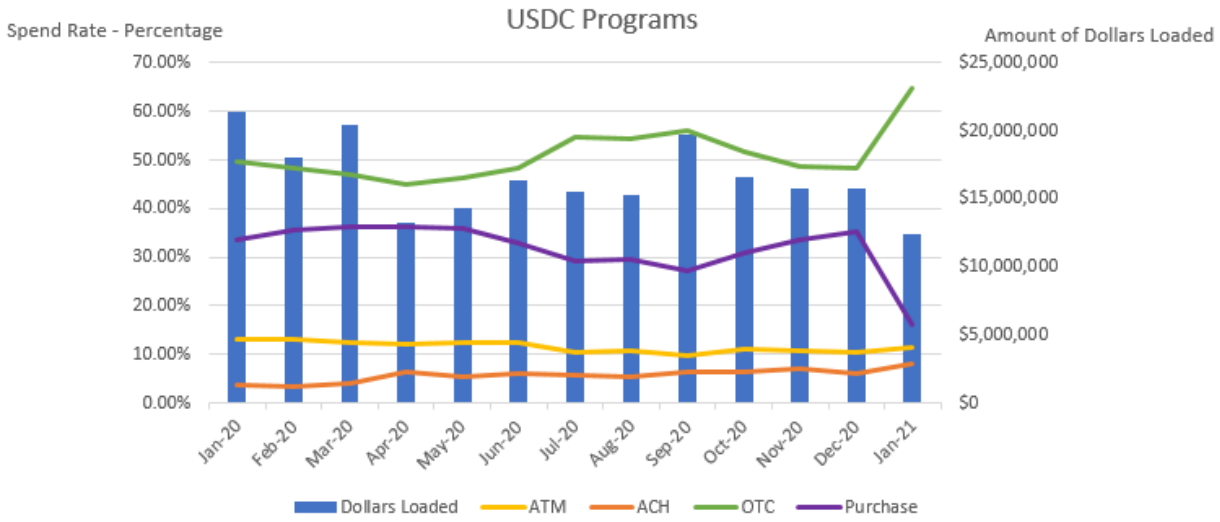
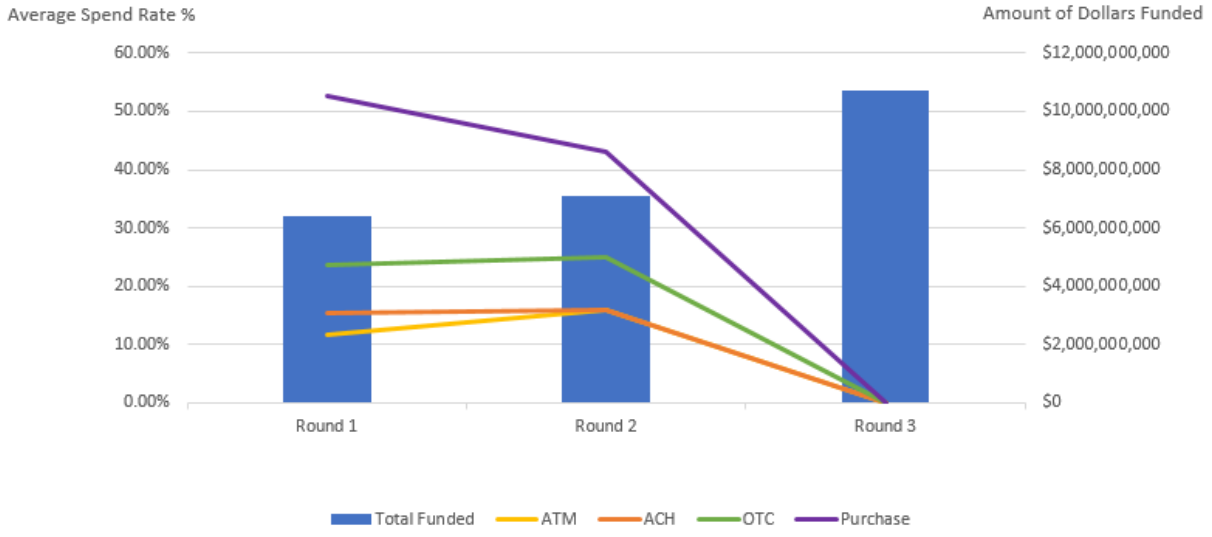


Chart J: Spend Rate – Large-scale program

Note: As of March 23, 2021, the chart below represents a large-scale program (i.e., stimulus payments) scenario related to average spending rate. For round 3 of stimulus payments, the average spending rate data is not available at this time.



Appendix D - Service Level Agreement

The FA shall meet, at a minimum, the following requirements. FA shall monitor on a monthly basis and report performance on a quarterly basis to include any necessary remediation steps.

Performance SLA	Requirement
Account Creation	• 98% within 3 business days of request
	• Remaining 2% within 5 business days
IVR	• 99% of calls answered on first ring
Customer Service Representative (CSR) Response Time	• 80% of calls within 30 seconds
	• 92% of calls within 90 seconds
	• 95% of calls within 180 seconds
Call Center Abandonment Rate	• No more than 5% if calls abandoned
Chargeback and Dispute Processing	• 100% acknowledged within 10 business days
	• 100% complete within 45 calendar days for ATM related claims
	• 100% complete within 90 calendar days for all others
Mailing of Paper Statements	• 95% by the end of third business day
	• Remaining 5% by end of fourth business day
Federal Agency Customer Service	• 99% uptime
System Availability for Transaction Processing	• 99% uptime
Batch File Submission	• 99% uptime
Report Availability	• 99% in timely and accurate manner

Incident Notification	• Notified within 24 hours of identification of incident
PII Incident Notification	• Notified within 1 hour of identification of incident

Appendix E - 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 (US) 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 US; 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 US 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 an Fiscal Service function, and criminal penalties may be imposed upon the officers or employees of Fiscal Service when the violation concerns the

[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.

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. For the first 60 days of user access, reviewing and signing the Rules of Behavior is adequate for meeting the security awareness training requirement. If the security awareness training requirement is not completed within the first 60 days, access may be revoked. 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.

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
- NIST Privacy Framework
- NIST SP 800-37
- NIST SP 800-53[2]
- 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

[2] Financial Agent can map NIST SP 800-53 controls to industry frameworks such as PCI-DSS.

- 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

Appendix F - Fiscal Service Policy for Financial Agents – Data Breaches of Sensitive Information

The compromise of sensitive information can result in significant risk of identity theft, harm and loss for individuals and businesses. It can also result in a loss of public confidence in government. To address this potential problem, Fiscal Service has developed a policy to address breaches of sensitive information[3] that may occur at a financial institution in its performance as Treasury's financial agent while handling Fiscal Service data. This policy sets forth the procedures that are to be followed in the event that sensitive information obtained or maintained as a financial agent or a contractor of a financial agent is the subject of an actual or suspected unauthorized access, use, disclosure or loss (hereafter referred to as an "incident").[4] It is our plan to monitor the reporting of these incidents, evaluate its impact on the Treasury and its financial agents, and then refine our policy/procedures as necessary.

Fiscal Service is aware that financial institutions are already subject to various rules established by bank regulatory agencies covering the real or suspected breaches of sensitive information. Fiscal Service does **not** intend to add to or impact any of those rules that address breaches of any customer data that is obtained or maintained outside the process of providing Fiscal Service-required services.

---

[3] Sensitive information includes Controlled Unclassified Information, as defined by NARA, Personally Identifiable Information as defined by OMB and Sensitive But Unclassified Information as defined under the Treasury Security Manual (TDP 15-71). For purposes of this policy/letter, these definitions are restricted to information obtained or maintained while performing services as a financial agent handling U.S. Government data. (See attachment at end of this policy).

[4] These procedures supersede any prior directions from Fiscal Service regarding the reporting of incidents involving sensitive information. Any prior instructions regarding the reporting of other processing or production issues that do not involve sensitive information are not affected by this letter.

Under this policy, financial institutions that perform financial agent services for Fiscal Service are subject to the incident reporting requirements summarized below, which are based, in part, upon standing Governmentwide guidance from the Office of Management and Budget (OMB). In addition to incident reporting, the OMB guidance outlines procedures for investigation, assessment and containment of security breaches. If an incident were to occur, Fiscal Service would look to the affected financial agent for appropriate assistance and support in carrying out an investigation. If an incident were determined to present a reasonable risk of identity theft, harm or loss, that institution may be called upon to work with Fiscal Service to notify affected individuals or businesses.

In addition, financial agents should safeguard all sensitive information obtained or maintained by the financial agent or its employees or contractors to accomplish Fiscal Service- required services. In handling sensitive information, financial agents should, at a minimum, comply with the procedures for the protection of customer information set forth in the Federal banking agencies' "Joint Interagency Guidelines Establishing

Information Security Standards," as may be amended from time to time. The financial agent may disclose sensitive information only to those employees of the financial agent who have a legitimate need to know the information to assist in the proper performance of Fiscal Service-required services. Furthermore, any contractor used by the financial agent to provide services under this agreement must agree in writing to the required safeguarding obligations consistent with those of the financial agent.

Incident Reporting to Fiscal Service:

OMB requires Federal agencies to notify US-CERT, the federal incident handling center located within the Department of Homeland Security, of any actual or suspected breach of "personally identifiable information." Under the OMB requirements, any employee of a Federal agency who learns of an actual or potential breach must notify appropriate agency personnel as soon as practicable; the agency must then report the breach to US- CERT within one hour of notification. The Department of the Treasury (Treasury) requires a similar notification to security officials of breaches of "sensitive but unclassified information." As a result, Fiscal Service must report when: 1) an individual gains logical or physical access without permission to a federal agency network, system, application, data or other resource; or 2) there is a suspected or confirmed breach of personally identifiable information regardless of the manner in which it might have occurred.

To support the foregoing, any financial agent employee or any employee of a contractor of a financial agent who becomes aware of an incident involving the possible loss, disclosure, misuse, or improper accessing of sensitive information must report the incident as soon as possible. The employee who becomes aware of the incident may report the incident internally through

whatever chain of notification that the financial institution may have established to meet the requirements of the bank regulatory agencies for data breaches. In any chain of notification, the financial agent management official who has been selected by the financial agent to contact Treasury must immediately notify the Fiscal Service IT Service Desk at 304-480-7777. The initial reporting of the incident within the bank and its subsequent reporting to Fiscal Service must be done as soon as possible so that Treasury is notified expeditiously of the incident. This applies to both the financial agent's employees and its contractor's employees. Additionally, Fiscal Service expects a financial agent and its contractor(s) to designate adequate back ups for the employees in any chain of notification for contingency purposes.

In reporting the incident, the financial agent should adhere to the following guidelines:

- Report the incident ***as soon as possible***, even if that means reporting before or after regular business hours or on a weekend or holiday.
- Do not delay reporting to confirm that a suspected incident actually occurred. Do not wait to get the "full picture" or have a proposed solution before reporting the incident.
- Do not delay reporting an incident because the incident seems harmless. If an incident occurs that does not appear to present any risk of harm or loss, or if there is a loss or breach of information but it is unclear whether the information constitutes personally identifiable information or sensitive but unclassified information, contact the Fiscal Service IT Service Desk at 304-480-7777 to confirm that reporting is not required.
- Report all incidents regardless of whether the information that may have been compromised is in electronic or paper form.
- The management official of the financial agent who is responsible for notifying Fiscal Service of a particular incident must speak to a representative at the Fiscal Service IT Service Desk. It is not sufficient to leave a voicemail message or to send an email.
- In addition to reporting the incident to the Fiscal Service IT Service Desk, the financial agent must notify the appropriate Fiscal Service Program Director. If the incident is in connection with the financial agent's capacity as a TGA bank, then notify the Treasury Support Group at the St. Louis Federal Reserve Bank.
- The financial agent should continue reporting status updates as requested by the Fiscal Service Program Director.

A few examples of incidents (as defined earlier) that could occur and must be reported are:

- The loss or theft of a computer, mobile device or media storage device (such as a thumb drive or disk) that contains or may contain sensitive information.
- The loss or theft of documents, including handwritten notes, paper checks, reconciliation records, letters, or other paper records, containing sensitive information.
- The delivery of a letter, email or other communication containing sensitive information to the

wrong recipient,[5] unless the recipient is another depositary institution.[6]
- An event in which sensitive information is erroneously displayed on a web page to someone other than the person to whom the information relates.
- An incident in which a user of a Fiscal Service system gains unauthorized access to another user's account, or initiates an unauthorized transaction affecting the account.

Fiscal Service has determined that the following incidents do not have to be reported:

- Checks or Information (Electronic and Paper) Routed to the Wrong Depositary Institution or Federal agency:

Reporting is not required when a check or sensitive consumer information is misrouted to a depositary institution or federal agency other than the intended recipient, if the circumstances indicate that the depositary institution or federal agency has not distributed the information to a third party. However, if a check or sensitive consumer information is suspected of being lost, stolen or misrouted to a person or entity other than a depositary institution or federal agency, the incident must be reported.

Note: If the information is suspected to have been made available to an individual(s) inside any depositary institution or federal agency other than those authorized by those entities to handle such information, those cases need to be reported.

- Incidents related to Treasury Tax and Loan (TT&L) Accounts:

Because the information associated with a payment to a TT&L account is related to businesses only, and not individuals, any actual or suspected breach of such information does not need to be reported to Fiscal Service.

- Incidents related to Treasury General Account (TGA) and International Treasury General Account (ITGA) Services:

Incidents related to TGA or ITGA services need not be reported unless an actual or suspected breach occurs during the performance of TGA/ITGA- related courier service or as part of the

[5] A recipient may be an individual, company, organization or other entity, including a Federal agency.

[6] For purposes of this letter, depository institution is defined to mean a bank, savings bank, savings association, credit union or similar depository institution chartered under U.S. law or the laws of any state, including a U.S. branch or agency of a foreign financial institution.

dedicated transmission, display or storage of data related to TGA/ITGA collections.

Fiscal service recently implemented a policy that prohibits sensitive information on laptops or other mobile devices unless authorized by the Fiscal Service Chief Information Officer. We expect that each financial agent will also have a policy to determine internally when it is appropriate to place sensitive information on selected laptops and other mobile devices used by the financial institution (or any contractor) as our financial agent.

In addition, Fiscal Service policy requires that all sensitive information and data (related to financial agency services only) residing on remote access devices[7] be encrypted. Fiscal Service is requiring that employees of financial agents and employees of contractors of our financial agents abide by the same standard.

Investigation and Notification Following Determination that the Risk of Identify Theft, Harm or Loss Exists:

In response to security breaches reported by financial agents, Fiscal Service may on a case by case basis request the affected financial agent to investigate the breach and report to Fiscal Service detailed findings as to the cause and impact of the breach as well as the remediation taken. Depending on the severity of the incident, and/or if Fiscal Service is required by the Department of the Treasury, the financial agent may be requested to provide frequent progress reports on the investigation.

Liability for Breaches of Sensitive Information:
As determined by Fiscal Service after reviewing any investigation conducted by the financial agent, the financial agent may be liable and may be required to reimburse Fiscal Service **and any affected agency or individual** for any costs, expenses or damages which result from the fraud, theft, willful misuse or negligence of the financial agent or its employees or contractors with respect to the handling and maintenance of sensitive information. Upon notification of an incident, Fiscal Service, in its sole discretion, may direct the financial agent to implement a range of immediate and subsequent corrective steps. The financial agent's liability may include (but not be limited to) the costs of notifying affected persons and providing credit monitoring for a period as deemed appropriate by Fiscal Service depending on the severity of the circumstances.

Raising Awareness of Fiscal Service Policy:

Financial agents should ensure that all of their employees and their contractors impacted by this

[7] A Remote Access Device is any device that can connect to an organization's network from a distant location from the network's facility. Remote access implies that the device becomes a fully-fledged host on the network. Financial agent should determine which devices utilized by the financial institution, e.g. Blackberries, fit this definition.

policy receive the proper education and guidance as part of their implementation efforts.

Questions:

Questions regarding this policy may be emailed to the Bank Policy and Oversight Division at BPO@fiscal.treasury.gov.

Attachment A
Sensitive Information

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.

Sensitive But Unclassified (SBU) information is defined as any information that the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of federal programs, or the privacy of individuals that they are entitled to under the Privacy Act. In addition, this includes trade secret or other information protected by the Trade Secrets Act. This definition may include other information designated as sensitive as defined by other sources not mentioned above.
Information designated as Limited Official Use, Fiscal Service Privileged Information, and PII is deemed as SBU information.
Examples of sensitive information include but are not limited to the following:

- Financial and law enforcement information
- Contracts and acquisitions
- ADP economic related or Wire Transfer system development
- Sensitive or proprietary information used for reports/economic matters of the US government

- Wire transfer codes or verification tables
- Reports, reviews and surveys involving the security of Fiscal Service facilities and systems
- Data elements used by a business or other entity to access information or initiate transactions on a Federal system, such as a password, PIN, user number, account number, security code or access code

Personally Identifiable Information (PII) means any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. The following are some examples of PII:

- Social Security Numbers
- Driver's License Number
- Addresses
- Student Identification Number
- Bank Account Number
- Credit or Debit Card Number
- Financial Information
- Telephone Numbers
- Fingerprint, Voice Print, Handwriting or Photograph
- Educational Information
- Financial Transactions
- Medical History
- Criminal or Employment History
- Mother's Maiden Name
- Other identifying number or code

Appendix G – Definitions

Term	Definition
Agency	Federal agency participating in the USDC program.
Agency Funds	Funds that are credited to a debit card account or Agency Virtual Account, but which remain public money and are owned by the Agency. As public money, Agency Funds are not subject to state escheatment

	laws or garnishment and attachment orders. Agency Funds may be expended and accessed by payment recipients using debit cards and digital pay as authorized by the Agency. Agency Funds are not considered disbursed to the payment recipients until drawn down or spent by the payment recipients. Agency Funds allocated to a debit card account or Agency Virtual Account but not disbursed, remain the funds of the Agency and may be transferred back to the Agency funding account. In addition to any applicable Federal Deposit Insurance Corporation (FDIC) insurance, Agency Funds are secured by collateral in accordance with the requirements of 31 CFR Part 202. Consumer protections offered by card branding associations do apply to Branded Cards and Agency Virtual Accounts (for example, Card Association Zero Liability policies).
Agency Profile	Describes the technical set up of one or multiple profiles on the Financial Agents platform, which is necessary to effectively implement an Agency Program. The Financial Agent will implement profiles as needed to meet the intent of the Agency Program.
Agency Program	Describes the U.S. Debit Card and Digital Payment Program attributes for a particular Agency purpose, as agreed upon, in writing, by the Fiscal Service and Agency on a Memorandum of Understanding (MOU), and Fiscal Service and Financial agent on a Direction to Agent (DTA).
Agency Virtual Accounts	Virtual Accounts to which Agencies, on a one-time or recurring basis, credit Agency Funds for purchases approved by the Agency or made on the Agency's behalf, or for other Agency-approved purposes. Generally, an Agency Virtual Account (i) is established for use by an employee, contractor, or other eligible recipient; (ii) may be personalized or non-personalized; (iii) may or may not have MCC restrictions; and (iv) may be audited by the Agency.
Branded Card	U.S. Debit Cards issued with a brand logo (depending on the program, at the discretion of the Financial Agent). Branded Cards may be used with a personal identification number (PIN) or signature anywhere the applicable brand is accepted. All U.S. Debit Cards must be branded when possible, to ensure appropriate fraud protections and broad acceptance.
Cardholder Funds	Funds that are allocated to a debit card account and which are disbursed by the Agency when allocated. Upon card activation, Cardholder Funds are considered disbursed and are no longer public money, are owned by the cardholder, and are subject to state escheatment laws and garnishment and attachment orders. Upon activation, Cardholder Funds

	belong to the cardholder and cannot be recovered by the Agency, except when specifically authorized by Federal Law. Cardholder Funds are FDIC-insured and cardholders must be provided all of the consumer protections that apply to a payroll card account under Regulation E (12 CFR Part 205) unless and until the Consumer Financial Protection Bureau amends Regulation E to provide consumer protections to prepaid cardholders.
Consumer Funds	Payments that are (i) disbursed to an individual's personal bank or debit card account via ACH credit or Direct to Debit; or, (ii) credited to a Consumer Virtual Account. Payments credited to a Consumer Funds account are disbursed by the Federal government upon payment delivery. Consumer Funds are owned by the account holder and are subject to state escheatment laws and garnishment and attachment orders. Consumer Funds cannot be recovered by the Agency, except when specifically authorized by Federal Law.
Consumer Virtual Accounts	Virtual Accounts established by individual payment recipients to receive single or multiple payments upon notification of a pending eligible payment from an Agency. The individual owns the funds credited to the account and the account relationship is between the Financial Agent and the individual. The individual is not limited on purchases or accountable to the Agency for spending. All fees associated with Consumer Virtual Accounts are charged directly to the Consumer Virtual Account. A Consumer Virtual Account (i) is established by a payment recipient who is notified of a payment by the Agency; (ii) must not have any MCC restrictions; and (iv) may not be audited by the Agency.
Direct to Debit	Refers to a transfer of funds in which the originator of a payment transmits funds to an eligible account using the payment recipient's debit card number. All domestic bank accounts and prepaid debit card accounts are eligible for Direct to Debit funds transfers if they are linked to debit cards branded by major debit card networks.
Europay, MasterCard, and Visa (EMV) Cards	Cards that store data on an integrated circuit which allow chip and pin or chip and signature payment at an ATM or POS Device where available. All U.S. Debit Cards must be EMV capable.
Merchant Category Codes (MCC)	MCC are used to identify vendor types and restrict or allow purchases with Agency Funds as identified by the Agency. MCC restrictions are not available for Cardholder Funds and may not be imposed on Consumer Virtual Accounts.

Payment Recipients	Refers to recipients of non-benefit payments issued by a federal agency. This terminology in this document covers both recipients who receive payment via a debit card or digital payment.
Tokenization	Refers to a process that secures the transmission of payment transaction and other sensitive data.
Unbranded Card	U.S. Debit Cards issued without a brand logo. Unbranded Cards may only be used at automated teller machines (ATMs) and those point-of-sale (POS) devices that accept a PIN. Unbranded Cards will only be used when a Branded Card cannot support an Agency's requirements.
Virtual Account	U.S. Debit Card prepaid account that is established to deliver payments to support Digital Pay service as additional payment delivery mechanism or to transmit funds to an eligible account using the payment recipient's debit card number.
Wallet	An electronic system that securely stores payment, transaction, and other information to enable an authorized user to initiate purchases and make payments.