# Requirements for Applications to Provide Prepaid Debit Card Services (updated 11/29/18)

## Table of Contents

## I. Overview

The Bureau of the Fiscal Service (Fiscal Service) is the bureau within the U.S. Department of the Treasury responsible for disbursing federal benefit 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 the Financial Management Service) 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. Treasury is required by statute to ensure that individuals required to receive Federal payments by EFT have access to an account at a financial institution "at a reasonable cost" and with "the same consumer protections with respect to the account as other account holders at the same financial institution." See 31 U.S.C. 3332(f)(i)(2). The Direct Express® card was created by the Fiscal Service to meet the requirement for a reasonable cost account while also addressing the particular needs of those federal benefit recipients who do not have (and may never have had) bank accounts.

Pursuant to its authority under 12 U.S.C. §§ 90 and 265, 31 C.F.R. §§ 202 and 208, and other applicable federal laws, the Fiscal Service seeks to designate a qualified financial institution as a Financial Agent to provide services necessary to operate the Direct Express® debit card program. The Fiscal Service recognizes that financial institutions may choose to provide some of the required services through partnership with other service providers. The Fiscal Service encourages interested financial institutions to consider partnering with or contracting with minority-owned or women-owned financial institutions and other businesses to assist in providing the required services.

Fiscal Service sponsors the Direct Express program and specifies the card features and fees. However, the Financial Agent issues the cards and holds the legal account relationship with the cardholder. Once Fiscal Service disburses payments to Direct Express accounts, the funds belong to the cardholder and not the government. The Financial Agent is liable for any unauthorized use of Direct Express cards that it cannot recover from cardholders under Regulation E or the card association rules.

## II. Timeline for Selection

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

| Date | Event |
|---|---|
| Nov. 27, 2018 | Fiscal Service issues announcement seeking applications |
| Feb. 15, 2019 | Application submissions due to the Fiscal Service (5:00 p.m. ET) |
| Mar. 8, 2019 | Fiscal Service notifies finalists |
| Mar. 11 – Apr. 19, 2019 | Fiscal Service sends sample Financial Agency Agreement to finalists; Finalists invited to make oral presentations if applicable; Fiscal Service review period |

| | |
|---|---|
| Apr. 26, 2019 | Fiscal Service selects Financial Agent(s) |
| May 10, 2019 | Selected applicant(s) signs Financial Agency Agreement |
| May 13, 2019 | Implementation planning begins |
| January 3, 2020 | Services under new Financial Agency Agreement begin |

## III. Projected Volumes

The Fiscal Service cannot predict the number of federal benefit recipients who will enroll in the Direct Express® program. As discussed in further detail below, in the event an applicant other than the incumbent is selected, the incumbent financial institution has the right to solicit existing Direct Express® cardholders to enroll in an account offered by the incumbent. It is unknown whether the incumbent will choose to do so and, if so, it is unknown how many cardholders would elect that option in lieu of continuing to participate in the Direct Express® program. In addition, it is unknown how many cardholders would elect to open a bank or prepaid card account at another institution for receipt of their federal benefit payments. In this regard, applicants should understand that in the event that a Financial Agent other than the incumbent is selected, existing Direct Express cardholders who do not establish a Direct Express account with the new Financial Agent will not have their benefit payments withheld and may request to receive their benefit payment by other means. Additionally, while it is possible that the Direct Express® program could be expanded to include additional types of federal payments, the Fiscal Service cannot guarantee that this will occur, nor can it predict the number of participants should this occur.

The Fiscal Service may determine that the services to be provided by the Financial Agent(s) selected under this solicitation will be limited to services pertaining to new Direct Express® enrollees only, that is, federal payment recipients who enroll in Direct Express® for the first time after the date the new Financial Agency Agreement goes into effect (or, in the case of the incumbent, to existing cardholders only). The Fiscal Service is providing historical Direct Express® statistical data in addition to references to Social Security Administration (SSA) data regarding the number of beneficiaries who have enrolled each year to date. This data is provided so that each applicant can draw its own conclusions about future Direct Express® enrollment volume. To date (through June 2018) there have been over 10.4 million cumulative enrollments to the Direct Express® card (this represents over 4.5 million open accounts). Those enrollment totals per year break down as follows:

2008: 262,189

2009: 593,466

2010: 700,493

2011: 1,300,856

2012: 1,536,301

2013: 1,589,015

2014: 1,116,742

2015: 1,036,126

2016: 916,552

2017: 954,322

2018: 473,080 (through June)

Of the total population of Direct Express® cardholders, the most represented group (over 52% percent) are the Supplemental Security Income (SSI) recipients. The next most represented groups are recipients of other SSA benefits and Veterans benefits. For a monthly statistical snapshot of SSA and SSI payments, including average dollar amounts, please visit http://www.ssa.gov/policy/docs/quickfacts/stat_snapshot/. For information about the number of various types of benefit payments disbursed by the Fiscal Service, see http://fiscal.treasury.gov/eft.

For estimates on the number of future SSA and SSI beneficiaries, actuarial data is available on the SSA website, http://www.ssa.gov.

**The Fiscal Service cannot and does not guarantee: (1) the number of cardholders who will remain enrolled or newly enroll in a benefit debit card program in the future; (2) the dollar amount that will be loaded onto benefit debit cards; (3) the number or types of transactions that cardholders will complete; or (4) any other information about expected cardholders, transactions, or expansions of the program that will occur in the future.**

## IV. 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, the Fiscal Service is authorized to designate a Financial Agent for the purpose of disbursing federal benefit payments electronically to debit card accounts. These statutory authorities and implementing regulations require that Financial Agents be financial institutions that meet certain requirements. Potential applicants are thus limited to financial institutions that meet the requirements described in 31 C.F.R. § 202. Notwithstanding this limitation, financial institutions may contract with other service providers including non-financial institutions such as processors or financial technology companies (FinTechs) to provide the services solicited in this document. The application must be submitted by the financial institution and the financial institution will have the legal relationship with the Fiscal Service and liability and responsibility to the Fiscal Service for any services provided by its contractors.

NOTE: The Federal Acquisition Regulations do not apply to the Financial Agent selection process.

The Fiscal Service will accept applications from financial institutions with the demonstrated ability to issue debit cards with the attributes described herein. Interested financial institutions must submit applications in accordance with the process described herein. The

Fiscal Service will review the applications and select one or more financial institutions to be finalists. Finalists will be invited to participate further in the Fiscal Service's selection process, which may include oral presentations and informal discussions. The Fiscal Service will provide finalists with the standard template Financial Agency Agreement that the selected Financial Agent(s) are required to sign. It is anticipated that the selected Financial Agent(s) will execute a final Financial Agency Agreement approximately two (2) weeks after the selection is made. The Financial Agency Agreement will be for a period of no less than five (5) years.

### *B. Evaluation of Proposals*

The evaluation of proposals will be based on multiple factors, and not solely on cost. As a threshold matter all applications must demonstrate an ability to meet or exceed all of the requirements set forth in this document and must comply with Section V, Application Submission Process. Applications that meet these requirements will be evaluated taking the following factors into consideration:

i. Experience in delivering prepaid debit card and/or EBT card services
ii. Benefits to the cardholder population
iii. Total program costs to the government over the life of the agreement, including, if applicable, the costs of transitioning the program to a new Financial Agent
iv. For applicants other than the incumbent, ability to transition the program in a manner than minimizes disruption to the program and to cardholders
v. Ability to innovate and implement innovative solutions that positively impact customer service and program efficiencies
vi. Ability to prevent, detect, and manage fraud without unduly disadvantaging cardholder access to funds and ability to transact on their accounts
vii. Experience and expertise of Key Personnel team

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

## V. Application Submission Process

Financial institutions submitting an application must comply with the following requirements. The 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 financial institution 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 titled "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- Qualifications, Section 2 – Pricing Proposal, etc.).

2. In addition to the 40 pages allotted to Parts I and II, the application may also contain a table of contents, pricing 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 financial institution would not want 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 financial institution may not submit any sales brochures, videos or other marketing information.

***B. Application Transmittal Letter.*** The application must contain a transmittal letter as described below:

1. The transmittal letter must be written on the financial institution's letterhead and signed by an official of the financial institution with legal authority to represent and bind the institution to the statements made in the application (faxed or scanned signatures are acceptable if the letter expressly states that the 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, and telephone number of the financial institution's contact person to whom the Fiscal Service will address all communications related to the Financial Agent selection process.

3. The transmittal letter must affirmatively state that the applicant (1) qualifies as a Financial Agent under 31 C.F.R. 202; (2) agrees to the selection approach described in this "Requirements For Applications to Serve as Financial Agent and to Provide Debit Card Services"; (3) understands that the selection process is not subject to the Federal Acquisition Regulations; (4) understands that the Fiscal Service makes no guarantees that the financial institution will be invited to participate further in the selection process; (5) understands that the Fiscal Service makes no guarantees regarding cardholder or transaction volume under a debit card program; and (6) understands that the Fiscal Service may decide to select a Financial Agent to provide services for the Direct Express® program in its entirely (existing and new enrollees) or only for new enrollees (or, in the case of the incumbent, only for existing cardholders).

***C. Part I of the Application.*** Part I of the application must address the following:

1. The applicant's qualification to act as a Financial Agent for the purposes described in this document pursuant to 12 U.S.C. §§ 90 and 265, and in accordance with the requirements set forth in 31 CFR § 202.

2. The identity of any partners, contractors, or affiliate organizations (collectively “partners”) with which the financial institution proposes to contract in order to provide the requested debit card services.

3. The capacity of the financial institution and its partners to issue Card Network-branded reloadable debit cards nationwide, and the maximum number of debit cards it could service.

4. The ability of the financial institution and its partners to establish reloadable and single load debit card accounts covered by FDIC insurance and compliant with the requirements of Regulation E (12 CFR 1005).

5. The ability of the financial institution and its partners to establish and staff a customer service center(s) with U.S. citizens or lawful resident aliens within the Continental United States. Applications must outline the financial institution's experience in customer service operations including the number of call centers operated, the number of calls/transactions per month handled, customer satisfaction ratings, and the years of experience.

6. The experience of the financial institution and its proposed partners issuing debit cards for recurring payments disbursed by a government or private entity including a clear and concise description of projects that illustrate the capabilities of the financial institution and its proposed partners, as well as information about the scope and length of each project described. In addition, the description should address experience the financial institution has in having to be flexible in making program (system, operational, managerial) changes to support a dynamic program.

***D. Part II of the Application.*** Part II of the Application must address or include the following:

1. **Qualifications**

a. **Security Compliance:** The applicant's ability to comply with all applicable security requirements of the U.S. Department of the Treasury, as specified in Treasury security directives. Among other things, Treasury directives require that employees who are working on this project, including call center(s) employees, must be U.S. citizens or lawful resident aliens. Appendix E contains sample Financial Agency Agreement security-related provisions for Direct Express®. The Financial Agent will not be operating an information system on behalf of the Fiscal Service.

b. **References:** The contact information of a reference for each of the benefit and payroll-like debit card projects for governmental or private entities described in Part I of the Application.

c. **Key Personnel:** Names, titles, business addresses, and experience of proposed key project personnel, including key personnel of any partners.

d. **Project Management:** How the applicant will manage the project. The applicant must submit a staffing chart describing how they will manage the project with a breakout of project functions.

2. **Pricing Proposal**

a. Cardholder Fees: In 2010 the Fiscal Service published a notice of proposed rulemaking (NPRM) at 75 FR 34394, requesting public comment on the fees, features and consumer protections associated with the Direct Express® card in light of the statutory requirements of 31 U.S.C. 3332. Following consideration of the comments, the Fiscal Service published a rulemaking that finalized the fees and features of the Direct Express® card and set forth the Fiscal Service's analysis that the low fees and nationwide availability of the Direct Express® card satisfy the statutory requirement of 31 U.S.C. 3332. See 75 FR 80315. Accordingly,

applicants must submit a pricing proposal that is based on maintenance of the existing cardholder fee schedule (see Appendix D), except to the extent that an applicant contemplates reducing or eliminating one or more of the existing fees. In direct support of this, it is also our expectation that cardholders will have access to a nationwide surcharge-free ATM network or other widely available no-cost means to access funds.

b. Compensation: We recognize that in light of the low fees, uncertainty regarding volumes, and the unique customer service needs and card usage patterns by the Direct Express® cardholder population (described below), the program may operate at a loss without additional compensation from Treasury. Therefore, pricing proposals should address financial compensation for operational costs based on assumptions that take into account both that the services to be provided cover all Direct Express® enrollees (i.e., current enrollees who choose to continue with the program plus new enrollees) and, for applicants other than the incumbent, that the services to be provided cover new enrollees only (the incumbent should assume that the services to be provided cover all Direct Express® enrollees or cover existing enrollees only). For each assumption, applicants should state how much, if any, compensation from Treasury is required and explain how that amount is calculated. Applicants may use any methodology for calculating required compensation – for example: per cardholder; one-time versus periodic; variable based on card usage; or other assumptions. Applicants 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, applicants should also provide a transparent and clear explanation of the rationale supporting that decision.

The information below is provided for consideration in your pricing proposal:

i. **Call Volumes**

**Table A: Monthly Call Volumes, July 2017 to June 2018**

| Month | Calls |
|---|---|
| July 2017 | 21,015,017 |
| Aug 2017 | 23,493,621 |
| Sept 2017 | 24,909,874 |
| Oct 2017 | 20,893,579 |
| Nov 2017 | 22,691,708 |
| Dec 2017 | 26,802,602 |
| Jan 2018 | 21,425,280 |
| Feb 2018 | 21,765,868 |
| Mar 2018 | 26,640,582 |
| Apr 2018 | 20,578,630 |
| May 2018 | 24,141,401 |
| June 2018 | 26,089,013 |

**Table B: Call Volumes for the First Three Days of the Month, July 2017 to June 2018**

| | Day 1 | Day 2 | Day 3 |
|---|---|---|---|
| July 2017 | 1,415,106 | 1,082,882 | 2,409,028 |

| | | | |
|---|---|---|---|
| August 2017 | 2,727,281 | 1,430,517 | 2,408,106 |
| Sept 2017 | 3,774,853 | 1,394,339 | 1,027,814 |
| Oct 2017 | 948,238 | 1,291,948 | 2,399,875 |
| Nov 2017 | 2,806,028 | 1,382,523 | 2,421,321 |
| Dec 2017 | 3,840,159 | 1,465,480 | 1,082,400 |
| Jan 2018 | 921,710 | 1,332,388 | 2,511,580 |
| Feb 2018 | 2,989,732 | 2,576,827 | 1,291,011 |
| Mar 2018 | 2,791,559 | 2,519,292 | 1,280,828 |
| Apr 2018 | 837,074 | 1,321,591 | 2,374,931 |
| May 2018 | 2,857,846 | 1,446,351 | 2,504,452 |
| June 2018 | 3,926,363 | 1,435,561 | 1,066,608 |

**Table C: Call Volumes for the Last Four Days of the Month, July 2017 to June 2018**

| | Day 28 | Day 29 | Day 30 | Day 31 |
|---|---|---|---|---|
| July 2017 | 493,168 | 422,674 | 452,867 | 989,001 |
| August 2017 | 610,316 | 673,246 | 770,952 | 1,182,195 |
| Sept 2017 | 886,598 | 2,487,388 | 1,101,349 | |
| Oct 2017 | 397,622 | 438,197 | 701,574 | 878,050 |
| Nov 2017 | 683,067 | 757,706 | 1,143,755 | |
| Dec 2017 | 1,003,735 | 2,680,109 | 1,186,170 | 989,001 |
| Jan 2018 | 493,168 | 422,674 | 452,867 | 1,182,195 |
| Feb 2018* | 610,316 | 673,246 | 770,952 | |
| Mar 2018 | 886,598 | 2,487,388 | 1,101,349 | 950,219 |
| Apr 2018 | 397,622 | 438,197 | 701,574 | |
| May 2018 | 683,067 | 757,706 | 1,143,755 | 878,050 |
| June 2018 | 1,003,735 | 2,680,109 | 1,186,170 | |

* February dates reflect Day 26, 27, and 28

**Table D: Calls Handled by Agents**

**CSR Calls: First Three Days and Last Four Days of the Month July 2017 to June 2018**

| | Day One | Day Two | Day Three | Last Days - One | Last Days - Two | Last Days - Three | Last Days - Four |
|---|---|---|---|---|---|---|---|
| July-17 | 32,812 | 21,911 | 45,607 | 14,793 | 8,054 | 9,096 | 26,701 |
| Aug -17 | 47,663 | 42,981 | 41,984 | 23,246 | 23,408 | 25,728 | 31,240 |
| Sep-17 | 50,589 | 30,181 | 21,737 | 20,211 | 22,779 | 37,668 | 23,203 |
| Oct-17 | 16,297 | 35,485 | 44,743 | 9,657 | 9,481 | 25,932 | 35,014 |
| Nov-17 | 45,619 | 41,196 | 35,790 | 24,285 | 25,034 | 26,527 | 34,727 |
| Dec-17 | 47,158 | 33,567 | 22,999 | 31,141 | 43,256 | 27,278 | 22,418 |
| Jan-18 | 28,581 | 44,356 | 49,274 | 11,106 | 26,178 | 28,675 | 39,727 |
| Feb-18 | 58,714 | 42,188 | 30,818 | 11,040 | 26,594 | 27,937 | 38,716 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Mar-18 | 56,502 | 43,546 | 31,358 | 30,715 | 37,649 | 53,847 | 36,794 |
| Apr-18 | 25,843 | 46,198 | 55,272 | 25,391 | 16,298 | 14,595 | 42,487 |
| May-18 | 47,182 | 39,472 | 41,195 | 11,257 | 24,426 | 24,930 | 32,989 |
| Jun-18 | 61,950 | 40,945 | 33,108 | 29,614 | 37,199 | 54,130 | 33,511 |

ii. **Card Balance Drawdown:** Direct Express® card financial transactions are not evenly distributed throughout the month. Financial transactions typically peak on payment days at the beginning of the month and are often compressed to certain time periods on individual payment days. This situation is further exacerbated when benefit payment days occur on a weekend or holiday and are combined to a single business day. Historical usage patterns have shown that during the first three days in any given month (covers benefit payments made on the 1st and 3rd of each month), the applicant should anticipate a significant amount of balance drawdown. Through the first six months of calendar year 2018, an average of nearly 67% of total deposits from the 1st of the month is withdrawn by the next day. Additionally, for the same time period, an average of 70% of total deposits from the 3rd of the month is withdrawn by the next day.

iii. **No Credit Check; Cardholder Retention:** Potential cardholders will not be subject to any credit screening requirements.

iv. **Relationship with Cardholder:** Once the funds are disbursed to a card, they belong to the cardholder and the applicant is responsible for liabilities associated with negative balances and fraud.

c. Transition Cost: 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 Direct Express® accounts from the incumbent to the applicant. See Subsection 3 below for more information regarding transition.

3. **Transition Plan:** Applicants other than the incumbent must submit a plan for transitioning existing Direct Express® accounts from the incumbent to the applicant. Applicants must be mindful that in many cases benefit payments received via the Direct Express® card are lifeline payments, and disruptions that result in any delay in receiving such payments are not acceptable. Thus transition plans must take into account and minimize, to the extent possible, any disruption to the program and to cardholders and must include contingency planning to address any operational or other issues that can occur during transition. 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, as well as an estimated timeline for completing the transition. The following information is provided to assist applicants in developing transition plans: the incumbent Financial Agent has the right to send a letter to existing Direct Express® cardholders informing them of the transition and providing cardholders with the option, in lieu of opening a new Direct Express® card at the new Financial Agent, to receive their benefit payments through another product offered by the incumbent or via a direct deposit account at the incumbent institution or another financial institution; cardholders who do not take these options or who take no action will be sent a new card; cardholders who receive a new

card will need to activate those cards; the entity activating the cards will be responsible for verifying the identity of the cardholder and will be liable for any fraudulent activations; identity verification may be difficult due to the limited availability of information regarding existing cardholders provided in public databases and by the Fiscal Service; multiple communications to cardholders may be required; and a high volume of telephone inquiries should be expected. Information about existing cardholders that will be made available to a new Financial Agent will include the cardholder's name (and, if applicable, the name of the representative payee); the cardholder's social security number (and, if applicable, the social security number of the representative payee); the most recent payment amount; and the most recent payment date. Other information such as mailing address and date of birth may be available for some cardholders. Transition plans should assume that the applicant will be responsible for sending new cards; activating those cards; communicating with cardholders, including locating those cardholders who were not reached via the initial communication (i.e., mailed notices returned as undeliverable); and fielding inquiries, and should address how each of these tasks will be performed including a communications plan to maximize outreach to existing cardholders. Alternatively, applicants may propose other transition approaches.

4. **Personnel / Infrastructure Capabilities:** A description of the personnel and infrastructure capabilities of the applicant to provide the required debit card services, including the security and privacy protection features. The applicant should take into consideration, as noted earlier in this document, that both customer service call volumes and Direct Express® card financial transactions are not evenly distributed throughout the month. Financial transactions typically peak on payment days at the beginning of the month and are often compressed to certain time periods on individual payment days. This situation is further exacerbated when benefit payment days occur on a weekend or holiday and are combined to a single business day. The applicant must demonstrate how, under these circumstances, extreme peaks of financial transactions and customer service requests are processed with no disruption to cardholders.

5. **Cardholder Educational / Public Relations Services:** The applicant must implement a financial education program designed to increase cardholder awareness of the features and benefits of the Direct Express® card. The applicant should provide a description of the type of marketing, education, and public relations services the applicant could support as part of their plan (e.g., web-based training, mobile education application, check stuffers, brochures, posters, advertising, customer surveys, social media, financial education rewards programs such as PayPerks). Marketing to Direct Express® cardholders for purposes not related to Direct Express® is prohibited.

6. **Media and Other Inquiries:** A description of the applicant's capacity to handle media and other high-profile inquiries regarding the Direct Express® program including a description of the resources available to handle such inquiries.

7. **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 and other necessary materials for program operations.

8. **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. Individually-owned accounts or if not, describe the account structure and how changes to the account structure impact the pricing proposal

b. FDIC insurance for cardholder funds

c. Must meet or exceed Regulation E protections for cardholders (describe protections that will be available)

d. The applicant must adhere to the existing Direct Express® card color scheme, trademark/logo, etc.

e. Whether the accounts will bear interest to the cardholder's benefit

f. A unique routing number(s) designated specifically to card accounts under the program; unique BIN(s) designed specifically for the program

g. Capability for personal identification number (PIN)-based or signature-based or other transactions at ATMs or POS devices, including ability to get cash-back at POS. Applicants should address capacity for the card to be used worldwide

h. Cardholder ability to withdraw funds at a bank or credit union branch or other ability to withdraw some or all funds off the card

i. Reloadability for purposes of receiving recurring federal benefits (cardholder will not be able to load personal funds to the debit card account)

Presently, federal benefit payments disbursed by the Fiscal Service are to be the only source of funding for Direct Express® card accounts. However, under certain circumstances, the Fiscal Service will direct the Financial Agent to accept payments from outside sources. This includes:

i. State Disbursed Supplemental SSI Payments. Some states supplement the federal SSI benefit with an additional payment. On certain occasions, a state may begin issuing the state's share of SSI payments directly rather than via SSA. State supplemental SSI payments must be allowed to post to Direct Express® card accounts in addition to the federal SSI payment. Close coordination is required between the applicant, the Fiscal Service, the SSA, and the state involved. For additional background information on state issued supplemental SSI payments, please visit, https://www.ssa.gov/ssi/text-benefits-ussi.htm

ii. Federal Non-Treasury Disbursed Payments. The applicant must accommodate and explain how it will process payments from benefit agencies that do not disburse payments through the Fiscal Service, otherwise known as Non-Treasury Disbursed Payments. Specifically, the applicant must describe how payment processing will be configured to accept ACH payments from a non-Treasury source.

Additionally, the Fiscal Service may consider allowing other payments disbursed by the Fiscal Service to benefit recipients (such as tax refund payments) to be loaded onto the Direct Express® card. Applicants should describe their capability to accept non benefit payments onto the card.

j. Cardholder's ability to use the card to pay rent and other bills, or to transfer money

k. Cardholder's name embossed on card

l. Card-related security features

m. Mobile application that will handle card management functions, such as the ability to check balances and track transactions

n. EVM/PIN and Chip capabilities for all cards

o. Access to funds to meet the special needs of cardholders who lose their cards and need immediate access to cash

p. Any other features that improve the customer experience and/or improve program efficiencies

9. **Innovation:** Applicants should describe their experience in innovation and provide specific examples either in connection with debit card programs or otherwise.

10. **Card Distribution / Management:** A description of the proposed process for issuing cards and managing issued cards. The description should address the following:

a. Enrollments:

i. Currently paying agencies and Treasury's fiscal agent, the Federal Reserve Bank of Dallas (FRB), receive the majority of new enrollments. New enrollments refers to the process that takes place when a federal benefit payment recipient first elects to receive their payments via Direct Express (see subsection b below). The applicant will, however, be responsible for re-issuing cards in situations such as the following: 1) a card has been lost or stolen, 2) the cardholder has experienced fraud on his/her account and needs a new card issued, or 3) expired cards. Applicants must describe how they will perform identity validation in such circumstances keeping in mind that some Direct Express® cardholders may not appear in commercially available databases. The applicant will assume no liability for fraudulent enrollments, except in those situations where the applicant took the fraudulent enrollment. See 31 Code of Federal Regulations Part 210.4(a). The applicant and the FRB will share fraudulent enrollment information to the extent legally permitted regardless of where the enrollment was initiated.

ii. Enrollments must allow, for single and/or representative payee beneficiaries, multiple benefits onto a single debit card, as well as payments for multiple beneficiaries onto a single debit card.

iii. Applicant may be expected to develop, in conjunction and coordination with the FRB, a web-based portal utilized for sharing and processing enrollment information between the two entities. This portal will allow FRB call center agents to enter enrollment data into the applicant's system, so that a debit card may be initiated in real time.

iv. Applicant may also interact with the FRB for the following:

- Development of a solution to distribute a potentially high volume of unsolicited prepaid debit cards that individuals can call to activate.
- Customer service issues. To resolve complex customer issues, the applicant will need to provide escalation options.

- The applicant may have further interaction with the FRB and the federal paying agencies as new agencies become eligible for Treasury disbursements and programs are added to further promote the growth of electronic funds transfers of federal benefit payments.
- Telephone cooperation that will include providing toll-free numbers for proper call routing of maintenance, lost/stolen, and enrollment status customer inquiries.
- Applicant resources may need to be provided to work in conjunction with FRB resources on specific projects.

v. Alternatively, applicants may propose to receive new enrollments directly without the involvement of the FRB. Applicants proposing to receive new enrollments directly should detail their plan for how they would receive and process new enrollments including how they would validate the identity of enrollees and should submit a pricing proposal.

b. New enrollments are currently processed as follows: There are two enrollment processes used for federal beneficiaries to enroll for the Direct Express card. Under one process, SSA uses a prenote to provide the Financial Agent with the information to set up card accounts, process card production, and mail cards to beneficiaries. Under the other process, the FRB uses a web-based portal to provide this enrollment information to the Financial Agent. The Financial Agent, through an Automated Enrollment Entry (ENR), provides to the federal payment agency routing and account information for assignment to the cardholder. Applicants will be expected to be able to receive and process such pre-notes and provide the ENR described herein.

c. Procedures for mailing cards to cardholders

d. How cards will be reissued when an existing card expires

e. How the applicant will define and handle "inactive" cards, for example, cards where there have been no deposits and/or withdrawals for a period of time, including how the applicant will handle the accounts of certain SSI payment recipients who may move in and out of the SSI program

f. Any alternatives to physical plastic cards (such as digital solutions) that meet the requirements herein including requirements related to security, privacy protection, and fraud prevention

g. Identity authentication ("customer identification procedures" or "CIP") procedures and compliance with the PATRIOT Act, Office of Foreign Asset Control and applicable Treasury regulations

h. 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

i. Cardholder activation and deactivation procedures, including how PINs are assigned and circumstances under which deactivation occurs

j. Payments to unpinned, inactive accounts. There will be circumstances where payments are made to card accounts that are never activated by the recipients. Applicants must address how they would identify these cases and return funds to the government in an automated way

k. The applicant must discuss how they can facilitate timely enrollments and proper timing of the issuance of their card to the recipient to prevent confusion and/or non-receipt of the subsequent payment. A Direct Express® card is mailed to a recipient after the paying agency receives and confirms a prenote transaction in order to prevent erroneous enrollments and to ensure that the recipient receives the card shortly before receipt of their next payment. It is imperative that the recipient does not receive the card too early, and therefore it is not funded on their subsequent payment, nor can the card be issued after funds were added to the card, and therefore the recipient misses their payment

l. Procedures and timeframes for re-issuing lost/stolen/destroyed cards:

i. Applicant will replace lost/stolen cards reported by cardholders in cases where the cardholder has a zero account balance and the fee for the replacement card cannot be collected until the cardholder's next payment is received (note: this applies to cases where the cardholder, per the fee structure, is required to pay for a replacement card).
ii. Applicant will return payments inaccessible due to a destroyed card through the ACH network.

m. Solutions for reducing the high volumes of lost and stolen cards through cardholder education or otherwise

n. If not already described, a description of the applicant's security and privacy protection procedures

11. **Card Funding:** A description of the applicant's proposed card funding (load and reload) procedures via the Automated Clearing House (ACH) network.

12. **Settlement Processing/Reconciliation:** The applicant must make funds available to settle to cardholders accounts at precisely 12am CT on the payment date as a significant number of cardholders begin withdrawing funds and engaging in POS transactions at that time (note that this is earlier than required under ACH Rules).

13. **Post-Payment Activities:** Processing federal government ACH payments presents some unique situations not typically experienced when processing traditional ACH payments. Among other things, a much higher rate of post-death reclamations occurs with respect to Direct Express® cards than with respect to prepaid cards generally, meaning that the issuing bank should consider the liability and workload arising from post-death benefit payments. Please see Appendix A to learn more about federal government post-payment activities. In addition, the regulatory requirements for processing federal government ACH payments can be found in 31 CFR Part 210 at:
https://fiscal.treasury.gov/ach and further explained in the
Green Book (Guide to Federal ACH Payments) located at:
https://fiscal.treasury.gov/reference-guidance/green-book.

The applicant shall provide a general description of its ability to meet the obligations outlined in 31 CFR Part 210, addressing such post-payment activities as: ACH non-receipts, ACH Returns, ACH reclamations, and Automated Enrollments (ENR), including both their current and future-state processes. Additionally, applicants should address their ability to communicate with SSA via a secured means regarding exception items, including returned and erroneous payments, non-receipt claims, and reclamations.

Below are volumes of non-receipt and reclamations activity for the program from 2016-2018:

Non-receipt

| Direct Express® ACH Non-Receipts, 2016-2018 | |
|---|---|
| 2016 | 16,827 |
| 2017 | 13,196 |
| 2018 (as of August) | 10,700 |

Reclamations:

| Direct Express® ACH Reclamations, 2016-2018 | |
|---|---|
| 2016 | 27,824 |
| 2017 | 27,817 |
| 2018 (as of June) | 29,814 |

14. **Garnishments:** Applicants must comply with 31 CFR Part 212.

15. **Set-Off:** A description of how the applicant's policies with respect to internal set-off for payment of cardholder fees, overdrafts, or other amounts owed by the cardholder to the applicant would apply to the proposed debit card product. Set-offs for amounts owed by the cardholder to the applicant for activity unrelated to the debit card product are prohibited.

16. **Cardholder Customer Services:** A description of how the applicant will meet Customer Service needs taking into account the particular needs of Direct Express® cardholders, including the need for customer service to be available at the time of payment to the Direct Express® card account. The description of the applicant's proposed cardholder customer services should include:

a. How a cardholder may obtain customer service by telephone (IVR, CSR), mobile application, text/email, online, or other innovative methods for communicating with cardholders

b. That the applicant agrees to make toll-free customer service available 24/7/365

c. What type of cardholder services will be available, including services related to lost/stolen cards, fraudulent or other unauthorized transactions, defective cards, obtaining balance and transaction information (including the availability of paper statements on request), and card usage questions

d. Whether cardholders will be able to obtain transaction and balance information via text messages, mobile phone applications, or otherwise

e. Availability of ATM network nationwide, including surcharge-free network and/or other ways cardholders may obtain cash nationwide and worldwide, and how the availability of a surcharge-free network and/or surcharge refunds to cardholders or other means of obtaining cash without fees impacts the applicant's proposed pricing structure

f. Access to customer service and new technologies to handle and process customer service needs by cardholders with disabilities, and availability of customer service in languages other than English

g. How the applicant will respond to cardholder disputes and agency claims of incorrect payments in compliance with appropriate ATM, Card Network association, and network operating rules

h. Training and competency requirements for customer service personnel

i. Quality control procedures the applicant uses to monitor and confirm that customer service requirements are being met

j. Availability of unique services that assist cardholders who are vulnerable (e.g., disabled, homeless, or unable to resolve card issues without the assistance of a paying agency employee). As background, vulnerable cardholders will be identified by paying agencies. The unique services will include the Direct Express® agent providing account information to a paying agency employee who is assisting the vulnerable cardholder with account issues or questions. These unique services are in addition to services the Direct Express® agent provides to typical cardholders. The applicant must be willing to enter into a Memorandum of Understanding (MOU) with the Social Security Administration. Please see Appendix B for additional information.

17. **Fraud Monitoring and Investigation:** A detailed description of how the applicant will prevent, detect, and handle fraud, including how the applicant monitors debit card activity for fraud; how the applicant will balance the needs of the elderly and disabled for lifeline payment access with the use of fraud detection and reduction; how the applicant will respond to card accounts that have been compromised and/or erroneous enrollments; security features of the card designed to prevent fraud and other fraud mitigation tools currently employed by the applicant; how cards are terminated; how incidents are investigated when the applicant believes fraud has occurred in connection with an account; and how quickly cardholders who are the victims of fraud can be made whole. Applicants must also include general information regarding incidents of fraud with respect to its other debit card programs and how those incidents are handled.

18. **Activity Reports:** A description of how and when reports are distributed, whether the report information can be broken down by payment types, as well as a description and samples of the types of reports that will be made accessible to the Fiscal Service including reports related to:

a. customer service call center activity

b. other customer service activity

c. aggregate funding activity

d. aggregate average daily balances

e. applicant's revenue fees by category and/or transaction type, including transaction fees (by transaction type), interchange fees, float earnings, issuer reimbursements, and other revenue or earnings

f. aggregate fraud activity

g. aggregate dispute activity

h. aggregate transaction activity

i. ad hoc reports including reports requested by the Fiscal Service.

The applicant must agree to participate in SSA's asset program (Access to Financial Institutions), and comply with all of the reporting requirements within that program. For more information please visit, https://www.ssa.gov/improperpayments/afi.html

19. **Customer Service to Government:** A description of the customer service and support that will be available to the Fiscal Service and federal program agencies whose beneficiaries are participating in the debit card program, including project management controls, assistance with 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 benefits eligibility status, enrollment status, and current card status (for example, account balance information).

20. **Service Level Requirements:** See Appendix C.

21. **Disaster Recovery/Risk Mitigation:** A general description of the applicant's emergency and disaster recovery plans.

22. **Contingency Plans:** A general description of the applicant's contingency plans in the event of systems failure or other similar event, including call center locations.

***E. Deadline:*** Applications are due on February 15, 2019. The Fiscal Service will send a confirmation of receipt by e-mail. The Fiscal Service may, in its discretion, accept applications and related materials received after the deadline.

***F. How to Submit Applications:*** Completed transmittal letters and Applications must be transmitted to the Fiscal Service by overnight or courier mail or by electronic mail. Only .pdf attachments will be accepted via electronic mail so that the documents cannot inadvertently be corrupted or modified in the transmission and downloading process. Applications must be submitted to:

*By hardcopy:*

Direct Express FASP
U.S. Department of the Treasury, Bureau of the Fiscal Service
401 14th Street, SW, Room 305B
Washington, DC 20227
Attn: Alicia Montgomery

*Electronically:*

Email to, Direct.ExpressFASP20@fiscal.treasury.gov

***G. Questions:*** Any questions regarding the Application submission process must be submitted to the Fiscal Service via e-mail at Direct.ExpressFASP20@fiscal.treasury.gov no later than February 8, 2019. The Fiscal Service will answer all questions as soon as possible and post questions and answers on http://www.fms.treas.gov/directexpressfasp14/index.html. Unless a financial institution is notified in writing that the deadline for submission has been extended, the financial institution must submit its Application by the deadline regardless of any outstanding questions it may have.

# Appendix A

**ACH Reclamations**:
ACH reclamations differ from commercial reclamations with regards to scope, liability and process. Specifically, the applicant is liable for ***all*** post-death payments, unless they meet the requirements to limit liability. Guidance on ACH reclamations is located at: https://fiscal.treasury.gov/reference-guidance/green-book/chapter-5.html

*Scenario:* 'Agency X' requests the Fiscal Service to recover ACH payments issued to Ms. Thompson after her death. 'Bank Y' sends a cashier's check to Fiscal Service to meet their obligation. The Fiscal Service processes the cashier's check and 'Agency X' is credited.

**ACH Non-Receipts**:
ACH non-receipts occur when a recipient claims non-receipt of a payment to the issuing agency. The Bureau of Fiscal Service investigates these claims cooperatively with the RDFI and provides status back to the issuing agency. Guidance on ACH non-receipts is located at:
https://fiscal.treasury.gov/reference-guidance/green-book/chapter-3.html

*Scenario:* 'Agency X' receives a claim of non-receipt from Ms. Jones regarding her refund payment. Fiscal Service contacts 'Bank Y' regarding the claim and determines that Ms. Jones payment posted to her savings account instead of her checking account. Fiscal Service advises 'Agency X' of the payment status and closes the claim.

**ACH Returns**:
All ACH Payments must be returned in accordance with NACHA Operating Rules when one or more condition is met (i.e., account closed, recipient deceased, etc.). If a federal Government payment cannot be posted according to the ACH entry, it is to be promptly returned and not held in suspense. Guidance on ACH Returns is located at:
https://fiscal.treasury.gov/reference-guidance/green-book/chapter-4.html

*Scenario:* Ms. Wells provides 'Agency X' with an incorrect account number at 'Bank Y' for her payment. 'Bank Y' returns payment to the Fiscal Service through ACH and 'Agency X' is credited.

**Post Payment Activities**:
Currently, the Fiscal Service conducts the majority of post-payment activities via paper format through the U.S. Postal Service. In the event of an update to an electronic format, the applicant will be expected to comply with both the legacy and electronic forms of post-payment processing.

# Appendix B

The selected applicant will be required to enter into a Memorandum of Understanding (MOU) with the Social Security Administration (SSA), under which the Financial Agent and SSA will exchange information regarding Direct Express® accounts of Title II and Title XVI beneficiaries, recipients and representative payees who manage those accounts on their behalf. The purpose of the MOU is to better enable SSA employees and the Financial Agent to assist card account holders whom SSA identifies as vulnerable (e.g., blind, deaf or subject to another disability; homeless; or who indicate they are unable to resolve account issues without the assistance of an SSA representative). The MOU supports a process to enable the exchange of information consistent with the requirements of the Right to Financial Privacy Act.

The MOU sets forth a process by which cardholders may authorize SSA and the Financial Agent to exchange information about their accounts, such as balance, transaction and payment history and card delivery status. This process does not replace the normal cardholder procedures for resolving disputes. It is a special procedure designed to be used on an exception basis for the benefit of individuals who have difficulty using the normal procedure. Under the procedure, an SSA representative provides a paper consent form for the vulnerable cardholder to sign to authorize the exchange of information over a period of no more than 3 months. SSA confirms the identity of the cardholder and retains the signed consent form for two years. SSA will provide the Financial Agent with the signed consent form upon request. SSA representatives must utilize a dedicated phone line designated by the Financial Agent, and SSA representatives must identify themselves using a security procedure agreed to by SSA and the Financial Agent.

# Appendix C

The table below illustrates the desired Direct Express® service levels that the Fiscal Service will monitor on a monthly basis.

| Performance SLA | Requirement |
|---|---|
| **Account Set Up within ENR review period** | ● 98% within 2 business days |
| | ● Remaining 2% within 4 business days |
| | |
| **Card Issuance** | ● 98% within 3 business days |
| | ● Remaining 2% within 5 business days |
| | |
| **Payments** | ● 99.97% within 1 business day |
| | ● Remaining within 2 business days |
| | |
| **IVR** | ● 99% of calls answered on 1st 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 |
| | |
| **CSR Call Quality** | ● 90% of CSR calls meet TBD standards |
| | |
| **Customer Satisfaction Survey** | ● 80% cardholders satisfied |
| | |
| **Fee Accuracy** | ● 99% accurately assessed |
| | |
| **Chargeback and Dispute Processing** | ● 100% acknowledged within 10 calendar days |
| | ● 100% complete within 45 calendar days for new acct, POS, foreign |
| | ● 100% complete within 60 calendar days |
| | |
| **Mailing of Paper Statements** | ● 95% by the end of 3rd business day |
| | ● Remaining 5% by end of 4th bus day |
| | |
| **ENR Transmission** | ● 99.9% verified deliverables were transmitted 1 business day later |
| | |
| **Web Administrative App** | ● 99% uptime |
| | |
| **System Availability for Transaction Processing** | ● 99% uptime |
| | |
| **Cardholder Access to Web Site** | ● 99% uptime |
| | |
| **Cardholder Access to Customer Support** | ● 99% uptime |
| | |
| **Batch File Submission** | ● 99% uptime |
| | |
| **Report Availability** | ● 99% in timely and accurate manner |
| | |
| **Incident Reporting** | ● Reported within 24 hours of occurrence |
| | |

# Appendix D

| Standard Free Services | |
|---|---|
| **Service** | **Fee** |
| Purchases at U.S. merchant locations | FREE |
| Cash-back with purchase | FREE |
| Cash from bank tellers | FREE |
| Customer Service calls | FREE |
| Web account access | FREE |
| Deposit notification | FREE |
| Low balance notification | FREE |
| Card replacement-One free per year | FREE |
| ATM balance inquiry | FREE |
| ATM denial of service | FREE |
| ATM cash withdrawal in the U.S. including the District of Columbia, Guam, Puerto Rico, and US Virgin Islands. Surcharge by ATM owner may apply. | One free withdrawal with each deposit to Direct Express® Card Account.* |

* For each federal government deposit to your Card Account, the fee is waived for one ATM cash withdrawal in the U.S. The fee waiver earned for that deposit expires on the last day of the following month in which the deposit was credited to the Card Account

| Other Services | |
|---|---|
| **Optional Service** | **Fee** |
| ATM cash withdrawals after free transactions are used in U.S. including the District of Columbia, Guam, Puerto Rico, and U.S. Virgin Islands. Surcharge by ATM owner may apply. | $0.90 each withdrawal (after free transactions are used) |
| Monthly paper statement mailed to you | $0.75 each month |
| Funds transfer to a personal U.S. bank account | $1.50 each time |
| Card replacement after one free each year | $4.00 after one (1) free each year |
| Overnight delivery of replacement card | $13.50 each time |
| ATM cash withdrawal outside of U.S. Surcharge by ATM owner may apply. | $3.00 plus 3% of amount withdrawn |
| Purchase at Merchant Locations outside of U.S. | 3% of purchase amount |

# APPENDIX E

## DirectExpress – Sample Financial Agency Agreement
## Information Security Provisions

## (Note – the DirectExpress Financial Agent will not operate any information systems on behalf of the Fiscal Service)

- **Location of Services.** Except as prohibited by law, the Financial Agent is hereby authorized to provide Debit Card services to cardholders within and outside of the United States as necessary to facilitate the use of Debit Cards by cardholders anywhere in the world. All other services provided under this FAA, including the development, operation and maintenance of systems and applications performed specifically and exclusively on behalf of the Treasury, shall be performed in the United States or its territories unless specifically authorized otherwise in writing. This restriction does not prohibit the use of offshore resources to augment software development, nor the use of foreign systems or other means of cardholder access to benefit payments. Except as necessary for benefit payment access, the Financial Agent will also ensure that all employees with access to systems, applications or other media that exclusively contain Treasury information are United States citizens or lawful permanent residents unless specifically authorized otherwise in writing.
- **Personnel Security.** The Financial Agent shall comply with the Fiscal Service Policy on Personnel Security for Debit Card Services dated October 11, 2007, (as may be amended), a copy of which is attached as **Exhibit 1**, as may be amended by time to time by mutual agreement of the parties (the "Policy"). Notwithstanding the foregoing, the Policy shall not apply to employees or contractors of the Financial Agent who may encounter information related to the Direct Express program (including cardholder information) in the ordinary course of their duties, except to the extent their duties are in furtherance of the services described herein.
- **Data Breach Policy**. The Financial Agent shall comply with the procedures set forth in the Fiscal Service Policy for Financial Agents re Data Breaches of Sensitive Information, dated October 5, 2007, (Fiscal Service Data Breach Policy), attached as **Exhibit 2**, regarding the loss, disclosure, misuse or unauthorized access to sensitive information, as defined in the policy statement. In the event that Exhibit 2 were to be amended after the Effective Date of this FAA, Financial Agent shall not be obligated to comply with any such amendment to Exhibit 2 unless and until the parties mutually agree to a written amendment to this Agreement.
- **Reviews and Audit.** Fiscal Service and entities authorized by Fiscal Service shall have the right to conduct announced and unannounced onsite and offsite physical, personnel and information technology testing, security reviews, and audits of the Financial Agent, and to examine all books and records related to the services provided and compensation received under this FAA, except as otherwise prohibited by Federal law. The Financial Agent shall be responsible for implementing corrective actions associated with such testing, reviews, or audits as directed by Fiscal Service. Because the Financial Agent is the issuer of the Debit Cards and holds the customer

relationship with the cardholder, the Federal Government will not be entitled to obtain or examine any records related to individual Debit Cards. Nothing in this FAA supplants or overrides the authority of any supervisory agency, including the Financial Agent's regulators, to examine or audit the Financial Agent or any aspect of the Direct Express program.

- **Liability.** In the event of a loss, disclosure, misuse or unauthorized access of sensitive information as defined in the Fiscal Service Data Breach Policy (**Exhibit 2**), which occurs as a result of the willful misconduct or negligence of the Financial Agent, Fiscal Service, in its sole discretion, may require the Financial Agent to pay the costs of notifying affected persons and providing credit monitoring services to them.
- **Liability for Costs of Investigation**. If Fiscal Service reasonably believes that the Financial Agent is in breach of this FAA, an investigation of the Financial Agent's actions by Fiscal Service or another entity may be required. If ultimately found to be in breach, the Financial Agent shall be liable for the reasonable costs and expenses of any such investigation to the extent that such costs and expenses are reasonably documented.

# APPENDIX E - EXHIBIT 1
## Fiscal Service Policy on Personnel Security for Debit Card Services dated October 11, 2007

The Financial Agent and its contractors shall comply with the following personnel security guidelines for employees who have access to Treasury enrollment and other personally identifiable information:

**1.** **Criminal Background Check.** As a condition of current and future employment, employees must be in compliance with Title 12, United States Code, Section 1829—no person shall work or have access to government information who has been convicted of criminal offences involving dishonesty, breach of trust, or money laundering.

**2.** **Hiring Approval.** Outside of Title 12, United States Code, Section 1829, the Financial Agent has the flexibility to hire and maintain individual employment. However, Financial Agent officials shall determine suitability, which includes an examination of conduct (adjudication) using information obtained through initial background screenings, employee declarations, documentation, and periodic reinvestigations.

**3.** **FBI Fingerprints.** This clearance must screen for felony/misdemeanor arrests and dispositions based on the subject's fingerprints. Fingerprints must be submitted to the FBI either electronically or by hard copy. If fingerprints are "unclassifiable," further inquiry by the FBI must be completed and results documented.

**4.** **Self Declaration Statement.** Each employee must complete and sign a Self Declaration Statement (statement) during the initial pre-employment background investigation and periodic reinvestigation. Financial Agent officials must require the subject to complete and sign this statement under the direct supervision of an appropriate Financial Agent official. At a minimum, this statement shall capture (and in certain instances reflect) the following:

(a) **Name.** Each employee must write his/her full legal name and other names used including nicknames, maiden name(s) and/or assumed names or aliases. This must be presented in such a way that each name category (i.e., full legal name, nicknames, maiden names, etc.) is addressed affirmatively by providing the appropriate name(s) or stating not applicable.

(b) **Seven Year Address History.** Each employee must provide a seven year work, school (if applicable) and home address history. Each work, school and home address must be full and complete and include the **county** associated with the address.

(c) **Criminal Question.** The statement must ask and the subject must answer the following question:

*Within the past seven years, have you been convicted of a misdemeanor or a felony (excluding minor traffic violations of $150.00 fine or less)?*

(d) **Reporting Obligation.** The subject must be made aware of his/her obligation to report information (i.e., criminal convictions, pending criminal charges and certain civil legal proceedings) that may have a bearing on one's initial or continued eligibility/suitability. The subject must be made aware of this obligation during the pre-employment process and during security awareness training sessions. Consistent with this requirement, the statement shall include the following language:

*I, _____(name) understand that it is my responsibility and obligation to fully and completely reveal during the pre-employment process and during active employment if hired, any matters, which may have an impact on my ability to have access to sensitive but unclassified (SBU) Government information and/or relevant equipment and/or systems. This includes, but is not limited to, revealing all new and/or existing criminal convictions or pending criminal charges, civil legal proceedings, delinquent financial obligations, and any matter involving breaches of honesty, integrity, and/or fiduciary duty.*
*I also understand that any matters discovered during any investigation that have not been previously reported by me may have an adverse impact on my ability to have access to SBU information and/or relevant equipment, and/or systems.*

(e) **Under Penalty of Perjury.** The signature line shall state:

*I declare under penalty of perjury that the information I provided in this self declaration statement is true, accurate and complete to the best of my knowledge and belief.*

**5. Social Security Number (SSN) Trace.** This process is multifaceted and involves authenticating information using a subject employee's SSN. Most private security vendors obtain this information through credit reporting agencies. Fraudulent use of SSNs and identity theft is a growing problem and this form of authentication is designed to detect fraudulent use. The SSN trace must include the following and documentation must be maintained to certify that all four components of the SSN trace are completed:

(a) **Aliases:** Authenticate that an SSN is associated with the subject and no one else including aliases, names of others using the SSN, and use of false SSN numbers,

(b) **Valid Range:** Authenticate that the subject's SSN, as issued by the SSA, falls within a valid range based on verification of the year and state the SSN was issued in,

(c) **Death File:** Authenticate that the subject's SSN was never issued or was/was not used in a death report or is part of SSA's deceased file record,

(d) **Addresses:** Authenticate that the subject's seven year self reported address history(s) vis-à-vis his/her Self Declaration Statement is consistent with other records. Any discrepancies between the subject's self-reported addresses, and other information, must be investigated.

**6. Government Issued Photo I.D.** Financial Agent officials must request and maintain a copy of the subject's government issued photo identification (I.D.), such as a driver's license. At the time of presentation by the subject the photo I.D. must be non-expired. The primary reason for requiring I.D. is to assist with establishing identity; thus, this requirement is not subject to periodic reinvestigation.

**7. Pre-employment.** Personnel security screenings must be completed and adjudicated prior to granting an employee staff-like access to facilities, sensitive but unclassified (SBU) information and security systems.

**8. Periodic Reinvestigation**

(a) **Full-Time Employees.** Any employee designated as full time, or maintains a regular and routine work week of at least 35 hours, shall be subject to a periodic reinvestigation inclusive of having primary screenings refreshed every five years.

(b) **Part-Time Employees.** Any employee designated as part time, temporary, seasonal, or lacking full-time status (less than 35 hours per week) shall be subject to a periodic reinvestigation inclusive of having primary screenings refreshed every three years.

**9. U.S. Citizenship/Lawful Permanent Residency (LPR)**

(a) **Establishment.** The establishment of U. S. Citizenship or LPR status is applicable to those employees who are subject to the standard screening requirement. The establishment of U. S. Citizenship or LPR status may also be applicable to individuals cleared under the baseline screening requirements if the Government expressly imposes a broader scope pertaining to U. S. Citizenship or LPR status. Documents that support an individual's claim of U.S. Citizenship/LPR status must be copied and retained. The completion of an I-9 alone is insufficient to meet this requirement since the I-9 addresses the employment eligibility of citizens, non-citizens, and non-permanent residents.

(b) **Citizenship.** Documents that support a claim of U.S. Citizenship include:

i. Birth Certificate issued by a state, county, parish, or city within the United States or one of its territories

ii. Birth document issued by a hospital within the United States or one of its territories

iii. U.S. Passport, current or expired

iv. Certificate of US Citizenship (INS form N-560 or N-561)

v. Certificate of Naturalization (INS N-550 or N-570)

vi. Report of Birth Abroad of a Citizen of the US (Department of State, FS-240)

vii. Certificate of Birth (Department of State, FS-545)

viii. Certificate of Report of Birth (Department of State, DS-1350)

ix. American Indian Tribal Birth Document

(c) **Lawful Permanent Residency.** A claim of Lawful Permanent Residency must be substantiated by a Permanent Resident Card (Card # I-551). The I-551 is valid for a 10 year period. A photo copy of the I-551 must be retained and copy must include the name, any numbers and dates, including the expiration date of the card.

**10. Security Awareness Training Certification**: Proof of security awareness training or a certificate that summarizes the training topics must be completed and maintained immediately after the training is provided. In addition, the certificate must provide the date of training, name of trainer, name and job title of the person being trained. Both the trainee and the trainer need to sign and date the training certification.

**11. Signed Non-Disclosure Statement.** All employees, including those subject to the security screening requirements, visitors, government officials, and others who require escort to sensitive areas must sign a non-disclosure statement as authorized by FISCAL SERVICE. This statement must certify that the signatory understands applicable security protocol and/or procedures and address penalties associated with unauthorized disclosure of information even after employment/affiliation/visit has ended. Authorized FISCAL SERVICE employees such as program and security personnel are exempt from this requirement.

**12. Exit Debriefing/Non-Disclosure**: In addition to any other process or procedures relative to employment resignation or termination, the debriefing process must include guidance and signed statements, which outline penalties associated with unauthorized disclosure of SBU information and any other programmatic, operational, and/or security related information that they had knowledge of, or access to. The departing employee must be made aware of his or her responsibility not to disclose information pertaining to processing operations.

**13. General Adjudication Principles**

**(a)** **No Delegation.** Information obtained via screenings through security vendors or other sources on any individual employee must be reviewed, weighed and judged by an employee of the Financial Agent who is experienced in personnel security adjudication. The Financial Agents shall not delegate adjudication responsibilities to a contractor or other non-employee.

**(b)** **Suitability.** Financial Agent officials shall conduct adjudications for suitability determinations using criteria that are established by the Financial Agent. If requested, the Financial Agent must be prepared to share procedures related to suitability and be prepared to defend to Fiscal Service hiring decisions based on screening results and adjudication procedures.

**(c)** **Justification.** Decisions made by adjudicators need to be documented. This is particularly important when there is different information from the same or different sources that needs to be reconciled, or when exceptions are made to Financial Agent standards or policy involving the suitability of the subject employee.

**14. Documentation of Employee Investigation**

**(a)** **Documentation/Retention:** The Financial Agent shall retain all documentation related to the investigation of each employee required under this policy. This documentation should be maintained separate and apart from personnel records.

**(b)** **Inspection:** Employees must be made aware that all information contained in their Treasury Folder is subject to Treasury inspection and that information is subject to reinvestigation.

**15. Authorized Access.** Access to operations and/or information must be controlled and is limited to employees including authorized contractors and vendors. Authorized access includes authorized Fiscal Service employees such as program and security personnel.

# APPENDIX E - EXHIBIT 2

***Fiscal Service Policy for Financial Agents re***
***Data Breaches of Sensitive Information dated October 5, 2007***

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[1] 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").[2] 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.

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

---

[1] Sensitive information includes Personally Identifiable Information as defined by OMB in its July 12, 2006, memorandum 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).

[2] 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.

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' Help 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 backups 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, Blackberry 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,[1] unless the recipient is another depositary institution.[2]
- 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.

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

[2] 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.

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

**Remote Access Devices[1]:**

Fiscal Service recently implemented a policy that prohibits sensitive information on laptops or other mobile devices unless authorized by 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 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

[1] 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.

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 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 BMT@Fiscal.Treasury.gov

## APPENDIX E - EXHIBIT 2 - Attachment 1
## Sensitive But Unclassified Information

**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:

1. Financial and law enforcement information
2. Contracts and acquisitions
3. ADP economic related or Wire Transfer system development
4. Sensitive or proprietary information used for reports/economic matters of the US government
5. Wire transfer codes or verification tables
6. Reports, reviews and surveys involving the security of Fiscal Service facilities and systems
7. 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:

1. Social Security Numbers
2. Driver's License Number
3. Addresses
4. Student Identification Number
5. Bank Account Number
6. Credit or Debit Card Number
7. Financial Information
8. Telephone Numbers
9. Fingerprint, Voice Print, Handwriting or Photograph
10. Educational Information
11. Financial Transactions
12. Medical History
13. Criminal or Employment History
14. Mother's Maiden Name
15. Other identifying number or code