FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Threshold Analysis (PTA) and/or Privacy Impact Assessment (PIA)

for

JP Morgan Chase Travel Card

(JPMC-TC)

Date Approved by Chief Privacy Officer (CPO)/Designee: 11/1/2018

PTA/PIA TEMPLATE VERSION 1.9 – August 2017

SECTION I – OUTSOURCED INFORMATION SERVICE DESCRIPTION

1. Describe the outsourced service and its purpose.

The JP Morgan Chase Travel Card (JPMC-TC) is a non-application that is used by the Federal Deposit Insurance Corporation (FDIC) to manage activity on the JPMC travel credit card. The JPMC institution operates as an outsourced service handling all aspects of credit card approval, authorization, and processing actions. The JPMC institution is insured, but not regulated, by FDIC. JPMC follows governmental security guidelines associated with the master contract through the General Service Administration (GSA) for protecting and safeguarding sensitive personally identifiable information (PII). The system of records notice (SORN) and related Privacy Act information can be found on the GSA website at: https://www.gsa.gov/reference/gsa-privacy-program/system-of-records-notices-sorns-privacy-act

FDIC employees initiate the process by completing an application for a corporate travel credit card and submitting it to the FDIC Division of Finance (DOF) Travel Services Section (TSS) email box. The application requests personal information about the employee, such as full name, home address, Social Security number (SSN), and other PII elements specified in Section II. TSS reviews the application for accuracy and manually enters it into JPMC PaymentNet, an encrypted web application, for processing by JPMC. Once the application is processed, JPMC sends the physical card to the home address listed on the employee's application.

FDIC employees may create an account in PaymentNet to manage their travel credit card accounts, including viewing transactions, disputing charges, viewing and printing monthly statements, and making payments. Employees may also provide their banking information for submitting payments via PaymentNet. TSS also utilizes PaymentNet for FDIC travel card oversight management and credit card usage reporting, including generating/obtaining reports, reviewing online inquiries, and adding/updating FDIC employee traveler information and user accounts. Refer to Section II for more information.

SECTION II – DATA TYPE, SOURCES, AND USE

2. Describe all information/data that will be collected, used, maintained or generated by the Outsourced Provider (Vendor) as part of the services provided under the contract. If no information/data is involved, select Not Applicable.

JPMC collects or receives the following PII about FDIC employees who complete an application for an FDIC-sponsored travel card: Name, SSN, Employee Identification Number (EIN), home address, home and mobile phone numbers, date of birth, country of citizenship, mother's maiden name, and business contact information (address, telephone number, email address). In addition, the employee may choose to provide JPMC with banking information (credit card number and full name) for submitting payments via PaymentNet. Refer to Question 7 for more information.

Note: In the event that an employee wants to change their name and receive a replacement travel card, the employee emails the request to DOF TSS, attaching any pertinent legal documentation such as a copy of their marriage certificate, divorce decree, driver's license, or Social Security card. DOF reviews the documentation provided by the employee and then sends the name change request to JPMorgan Chase via email. However, the documentation provided by the employee is not shared with JPMorgan Chase. JPMorgan Chase relies on DOF to review the documentation and

submit the request on behalf of the employee. DOF does not retain the documentation provided by the employee after processing the request.

3. Describe the intended purpose and use of the above information/data. If no information/data is involved, select Not Applicable.

The above information is used for the issuance and management of FDIC travel credit cards accounts, including approval, authorization, suspensions, terminations, and processing.

4. What types of personally identifiable information (PII) are (or may be) included in the information specified above? *(This is not intended to be an all-inclusive list. Specify other categories of PII, as needed.*):

PII Element	Yes	No
Full Name	☒	☐
Date of Birth	☒	☐
Place of Birth	☐	☒
Social Security Number	☒	☐
Employment Status, History or Information	☐	☒
Mother's Maiden Name	☒	☐
Certificates (e.g., birth, death, naturalization, marriage, etc.)	☐	☒
Medical Information (Medical Records Numbers, Medical Notes, or X-rays)	☐	☒
Home Address	☒	☐
Phone Number(s) (non-work)	☒	☐
Email Address (non-work)	☐	☒
Employee Identification Number (EIN)	☒	☐
Financial Information (e.g., checking account #/PINs/passwords, credit report, etc.)	☒	☐
Driver's License/State Identification Number	☐	☒
Vehicle Identifiers (e.g., license plates)	☐	☒
Legal Documents, Records, or Notes (e.g., divorce decree, criminal records, etc.)	☐	☒
Education Records	☐	☒
Criminal Information	☐	☒
Military Status and/or Records	☐	☒
Investigation Report or Database	☐	☒
Biometric Identifiers (e.g., fingerprint, voiceprint)	☐	☒
Photographic Identifiers (e.g., image, x-ray, video)	☐	☒
Other (Specify: country of citizenship and *business* contact information, including business address, business email address and business telephone number)	☒	☐

5. If Social Security Number (SSN) is checked in question 4, please answer the following:

a) Explain the business purpose requiring the collection of SSNs: SSN is collected for purposes of processing the credit application through JPMC. It is also used as a secondary key to be used for reporting activity. Refer to 5(b) for more information.

b) Provide the legal authority which permits the collection of SSNs.

12 U.S.C. § 1819

In addition, the Travel and Transportation Reform Act of 1998 (Public Law 105-264) and implementing GSA regulations mandate Federal government account holders to use government-issued travel charge cards for all official travel expenses and cash advances, unless they have an exemption. The application for a government-issued travel card requests SSN and other sensitive PII necessary for issuing the travel card and managing the travel account. Further, pursuant to Section 846 of the Consolidated Appropriations Act of 2006 (Public Law 109-115), agencies are required to assess the credit worthiness of first-time government travel account applicants prior to issuing them travel accounts. This assessment necessitates the collection of SSNs.

c) Identify whether the SSN is masked or otherwise truncated as part of the outsourced service: Yes, SSNs are truncated to the last four numbers in the NFE application and in the file that NFE sends to JPMC, but employees must provide their full SSNs during the application process for the business purposes described above. In addition, SSNs are masked in PaymentNet.

6a. Please provide an estimate of the number of records maintained by the vendor for this contract that contain PII:

Estimated Number of Records Containing PII				
0 ☐	1-500 ☐	501-1,000 ☐	1,001 – 2,500 ☐	2,501 – 5,000 ☐
5,001 – 7,500 ☐	7,501 – 10,000 ☐	10,001 – 50,000 ☒	50,001 – 100,000 ☐	over 100,000 ☐

6b. If "0" was answered for 6a, please explain[1]: N/A

7. What are the sources of data (both PII *and* non-PII) for the outsourced service/project? How is the data derived?

Data Source[2] (List all sources that the Outsourced Provider collects, obtains or receives data from, as part of the services provided under the contract.)	**Type of Data Provided by Source & How It is Derived** (Describe the type of PII and non-PII data provided by each source. If PII is included in the data, list the specific PII elements, and explain how the PII is derived.)	**Does Data Include PII?**
FDIC Employees	FDIC employees initiate the process by completing an application for a corporate travel credit card. The application requests the following information: name, SSN, EIN, home address, business email, business address, business telephone number, date of birth, mobile phone number, home phone number, country of citizenship, and mother's maiden name. The employee may also choose to provide JPMC with banking information (credit card number and full name) for payments via PaymentNet. The employee scans and submits the signed application, along with a FDIC Travel Card Program Certificate from Corporate University	☒ Yes ☐ No

[1] If the vendor has not received work to date for this contract and "0" is checked in 6a, please explain approximately how many records may be maintained by the vendor if they are awarded work under this contract in the future. Additionally, the Division responsible for this vendor must update this PIA to reflect the accurate number of records containing PII that the vendor maintains if this changes in the future.

[2] Examples of potential data sources include, but are not limited to: internal (FDIC) or external (non-FDIC) systems, websites, individual members of the public (e.g., customers, borrowers, etc.), FDIC employees, FDIC contractors, credit bureaus, commercial entities, public records, government agencies, etc.

	and an Employee Acknowledgement form, to the DOF TSS email box.	
FDIC DOF Travel Services Staff (TSS)	Authorized DOF TSS staff review employee travel card applications for accuracy and forward completed applications to JPMC via PaymentNet. TSS staff also manually enter the FDIC employee cardholder information from the new credit application (name, SSN, EIN, statement/card delivery address, home address, business email , business address, business telephone number, date of birth, mobile phone number, home phone number, country of citizenship, and mother's maiden name) into JPMC PaymentNet. TSS staff can also update existing FDIC employee user accounts, including address changes.	☒ Yes ☐ No
FDIC New Financial Environment (NFE) / Supplemental Payment System (SPS)	NFE sends a digitally signed Pretty Good Privacy (PGP) file via GlobalScape secure file transfer protocol (SFTP) to JPMC that contains new employee information necessary to establish travel cards, including employee name, EIN, and the last four digits of the SSN. The encrypted data files are loaded to PaymentNet by authorized JPMC staff. NFE also securely transmits employee payments and reimbursements to JPMC, including employee name and full credit card number. Specifically, NFE allows employees to designate a direct payment amount to their FDIC travel card account when submitting an expense report. The payment is disbursed to JPMC through SPS, an NFE module, via a secure virtual private network (VPN) tunnel. NFE must provide the full name and credit card number of the employee to ensure the payment is credited properly.	☒ Yes ☐ No

8. How will FDIC and/or the Outsourced Service Provider retrieve data or records as part of the outsourced service or project? Can data be retrieved using a personal identifier (e.g., name, address, SSN, EIN, or other unique identifier)?

Yes, EIN will be used to search and retrieve data.

9. In the Federal Register, under which Privacy Act Systems of Record Notice (SORN) does this system operate? Provide number and name.

FDIC 30-64-0012, Financial Information Management Records
GSA/GOVT-3, Travel Charge Card Program

This completes the PTA.

- Do not complete the rest of the form, if the service provider is not processing or maintaining sensitive PII. This is the case, if you checked:
  - NOT APPLICABLE for question 3 and NO for all items in question 4; OR
  - Only Full Name in question 4.

- Continue completing the remainder of the form, i.e., Sections III thru VI in their entirety (questions 10 through 18), if the service provider is processing or maintaining sensitive PII. This is the case, if you checked:
  - YES for Social Security Number (SSN) in question 4; OR
  - YES for SSN or for Full Name in addition to one or more boxes in question 4.

- If you have questions or are unsure about whether or not you should complete the remainder of this form, please contact your Division ISM or the Privacy Program Office (privacy@fdic.gov).

SECTION III – DATA ACCESS AND SHARING

10. In the table below, specify the systems/applications and parties (FDIC and non-FDIC) that will access or receive PII data as part of the outsourced service/project. ***(Check "No" or "Yes" for each category. For each category checked "Yes," specify who will have access to, be provided with, or maintain the PII, what PII elements will be accessed/shared/maintained by them, how the access or sharing will occur, and the purpose and use of this PII.)***

PII Will Be Accessed By and/or Provided To:	Yes	No	If Yes, Explain How and Why the PII Will Be Accessed/Shared
10a. FDIC Outsourced Service Provider (OSP) Staff; OSP Subcontractors; and/or OSP Systems	☒	☐	JPMC's website PaymentNet is used to process the credit application to establish the employee account. The PII specified in question 4 is used for approving the credit application, travel card processing and management of travel expenses. JPMC Administrators access PaymentNet for purposes of approving credit applications and reviewing accounts to resolve billing disputes or issues pertaining to travel expenses.
10b. FDIC Personnel and/or FDIC Systems/ Applications	☒	☐	**FDIC employees** may create an account in PaymentNet to manage their travel credit card accounts, including viewing transactions, disputing charges, viewing and printing monthly statements, and making payments. Upon approval of their travel card application, the employee must electronically accept the agreement via PaymentNet. **DOF TSS Staff** have access to PaymentNet to enter travel applications, which include the PII specified in question 4, and review accounts. TSS receive monthly reports via PaymentNet to review the status of employee accounts and resolve delinquencies.
10c. Individual Members of the Public (e.g., bidders, investors, borrowers, customers, etc.)	☐	☒	Not applicable.
10d. Other Non-FDIC Entities/ Parties and/or Non-FDIC Systems/Applications	☒	☐	Credit bureaus may receive PII for the purposes of establishing employee accounts and reporting non-payment.
10e. Federal, State, and/or Local Agencies	☐	☒	Not applicable.
10f. Other	☐	☒	Not applicable.

11. If data will be provided to, shared with, or maintained by non-FDIC entities (such as government agencies, contractors, or Outsourced Information Service Providers), have any of the following agreements been issued?

Data Protection and/or Sharing Agreements	Yes	No
FDIC Confidentiality Agreement (Corporation)	☐	☒
FDIC Confidentiality Agreement (Individual)	☐	☒
Non-Disclosure Agreement (NDA)	☐	☒

Memoranda of Understanding (MOU)	☐	☒
Information Sharing Agreements (ISA)	☐	☒
Authentication Risk Assessment	☐	☒
Other Applicable Agreement(s) (*Specify*: GSA Travel Master Contract)	☒	☐

If you answered NO to any item above, please provide additional information if available: JPMC TC is under the GSA Travel Master Contract. The contract requires that all Contractor personnel who have access to government or cardholder data sign a non-disclosure agreement, prior to having access to agency/organization systems (GSA SmartPay2 Master Contract, Section C.3.1.6 *Personnel Security).*

SECTION IV – NOTICE AND CONSENT

12. Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

☐ No. Individuals do not have the opportunity to "opt out" of providing their data and/or consenting to particular uses of their information. ***(Explain why individuals are not able to opt out (either for specific data elements or specific uses of their data.):***

☒ Yes. Individuals have the opportunity to decline to provide their personal data or to consent to particular uses of their information: The employee can decline to provide the PII necessary to establish the account. However, JPMC has the right to decline the application.

13. If PII is being collected via a public-facing website and/or application as part of this outsourced service, has the Outsourced Information Service Provider posted any of the following types of privacy policies or Privacy Act notices?

☐ No
☒ Yes *(If yes, check applicable box(es) below.)*
- ☐ Link to FDIC Privacy Policy
- ☐ FDIC Privacy Act Statement
- ☒ Contractor Privacy Policy or Statement
  https://www.jpmorgan.com/country/US/EN/privacy
- ☐ No Privacy Policy has been posted

☐ Not applicable

SECTION V – DATA SECURITY AND ACCURACY

14. Please assert what administrative procedures and technical safeguards are in place to protect sensitive PII data in the Outsourced Information Service Provider's care. *[Provide the name of the Outsourced Service Provider and check all applicable box(es).]*

☐ [Outsourced Information Service Provider name] [has gone/will go] through the security review required by the FDIC's Outsourced Information Service Provider Assessment Methodology to determine and/or verify their having appropriate physical, technical, and administrative security measures to safeguard FDIC-provided PII and other sensitive data. If it has gone through the Methodology, has it been approved? ☐ NO ☐ YES

☐ The FDIC conducts background investigations (BIs) on key [Outsourced Information Service Provider name] personnel and other applicable personnel prior to their beginning work on the contract.

☐ The [Outsourced Information Service Provider name] is subject to periodic compliance reviews by FDIC. Per the contract, scheduled and unannounced inspections and assessments of the Outsource Service Provider's facilities, personnel, hardware, software and its security and privacy practices by either the FDIC information technology staff, the FDIC Inspector General, or the U.S. General Accountability Office (GAO). These inspections may be conducted either by phone, electronically or in-person, on both a pre-award basis and throughout the term of the contract or task order, to ensure and verify compliance with FDIC IT security and privacy requirements.

☒ Other (Explain any other administrative and/or technical safeguards in place to protect PII data in the Outsourced Information Service Provider's care.) ***Attach the Contract Clause Verification Checklist to the back of this form.***

As previously noted, this contract is under the GSA SmartPay2 MasterContract. Following are excerpts from the contract related to key administrative and technical safeguards that are in place to protect the data.

C.3.1.7 Privacy and Security Safeguards: The Contractor shall ensure confidentiality of data. The Contractor shall follow federal Government-accepted security principles and practices per NIST SP 800-14, or better, to protect government information in the Contractor's infrastructure from disclosure to unauthorized persons. This protection shall include, but not be limited to, sensitive information maintained.

The Contractor shall protect the integrity of government and cardholder data, including, but not limited to the following:

- *The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government;*
- *To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases; and*
- *If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.*

C.3.1.6 Personnel Security: To ensure the security of government and cardholder information, the Contractor shall…[r]equire that Contractor personnel who have access to government data systems have, at a minimum, a background investigation that includes an acceptable result on Standard Form 85P Questionnaire for Public Trust Positions, or equivalent form…Performance under the task order(s) may require the Contractor to have access to information classified up to and including "Top Secret." Therefore, upon award, and as requested by the agency/organization, the Contractor shall obtain and maintain the appropriate personnel and facility clearances to have access to and custody of such information as specified by the agency/organization...

C.3.1.4 System Security Reviews and Audits: Program systems shall be subject to security reviews, as required by the Government, before and throughout the period of performance…The Government reserves the right to conduct onsite inspections as it deems appropriate…The Contractor is required to provide complete information and supporting evidence needed for the Government's detailed security control reviews, audits, and certification and accreditations of the Contractor's systems.

C.3.1.1 Security Plans: …The Contractor's security requirements/measures/standard procedures shall protect the integrity, security, and proper functioning of all databases and systems involved in the operation of the Government's card program(s). The databases and information processing systems containing government information shall have sufficient security measures to protect against deliberate or inadvertent loss, degradation, alteration, release, or damage of information. The Contractor shall be held responsible for any misuse or fraud resulting in information mistakenly released by the Contractor…

15. What are the procedure(s) for ensuring that the information maintained is accurate, complete and up-to-date? *[Check all applicable box(es) and insert the appropriate response and System/Project name.]*

☒ Data is collected directly from individuals and/or from the failed financial institutions. As such, the FDIC and its vendors rely on the individuals and/or financial institutions to provide accurate data.

☒ The vendor/contractor works with FDIC to verify the integrity of the data before, in conjunction with, and after inputting it into the system or using it to support the project.

☒ As necessary, an authorized TSS specialist checks the data for completeness by reviewing the information, verifying whether or not certain documents or data is missing, and as feasible, updating this data when required.

☐ Other (*Please explain*.)

16. In terms of assuring proper use of the data, please assert whether the following statements are true for the Outsourced Information Service Provider. (*Check all applicable box(es) and insert the name of the Outsourced Information Service Provider and title of the firm's senior management official.*)

☒ Within FDIC, the JPMC TC Program Manager/Data Owner, Technical Monitors, Oversight Manager, and Information Security Manager (ISM) are collectively responsible for assuring proper use of the data. In addition, it is every FDIC user's responsibility to abide by FDIC data protection rules which are outlined in the FDIC's Information Security and Privacy Awareness training course which all employees take annually and certify that they will abide by the corporation's Rules of Behavior for data protection.

☒ Additionally, the Outsourced Information Service Provider is responsible for assuring proper use of the data. Policies and procedures have been established to delineate this responsibility, and the vendor has designated JPMC Federal Card Services to have overall accountability for ensuring the proper handling of data by vendor personnel who have access to the data. All vendor personnel with access to the data are responsible for protecting privacy and abiding by the terms of their Non-Disclosure Agreements, as well as the vendor's corporate policies for data protection. Access to certain data may be limited, depending on the nature and type of data. (Refer to Section III of this Privacy Impact Assessment for more information on data access criteria.)

☒ The Outsourced Provider must comply with the GSA SmartPay2 Master Contract requirements related to incident response and incident monitoring, as detailed below.

C.3.1.1 Security Plans: …The Contractor shall submit quarterly security and fraud management reports as well as individual reports of security breaches and fraud incidents to the GSA Contracting Officer by no later than the 15th calendar day of the next fiscal year quarter. GSA will review these reports and keep track of security breaches and fraud incidents as a means of monitoring the effectiveness of the

Contractors' security practices. Based on the frequency, nature, and seriousness of security breaches and fraud incidents, GSA will assess the Contractor's security controls in the specific areas where breaches occurred and take action as appropriate. The Contractor shall implement standard procedures to be outlined in their security plan for reacting to fraudulent/questionable activity and security breaches including, but not limited to, the following:

- *Immediately notifying the agency/organization point of contacts (OPCs) and cardholders when their accounts are compromised;*
- *Assigning new account numbers to accounts that are compromised;*
- *Providing additional monitoring for accounts that are known to have been compromised; and*

Regardless of the impact on the program, the Contractor shall immediately notify the designated agency/organization point of contact of any security breach that the Contractor experiences.

☐ None of the above. *(Explain why no FDIC staff or Outsourced Information Service Provider personnel have been designated responsibility for assuring proper use of the data.)*

SECTION VI – DATA RETENTION AND DISPOSAL

17. Where will the Outsourced Service Provider store or maintain the PII data identified in question 4? Describe both electronic and physical storage repositories, as applicable.

The PII will be maintained and stored in JPMC PaymentNet.

18. Specify the period of time that data is retained by the Outsourced Service Provider and the specific procedures for disposing of or returning the data at the end of the retention period or contract, whichever is first.

Per SmartPay2 Master Contract: In addition to the record retention requirements of FAR 4.703, the Contractor shall serve as the Government's agent for document repository as it relates to all transactions under the card program(s). The Contractor shall maintain electronic records of all transactions that exceed $25,000 for a period of 6 years and 3 months after final payment, and for all transactions of less than $25,000, for a period of 3 years after final payment. Final payment is defined as the final payment for the particular charge under each agency's/organization's task order. The Contractor shall segregate this transaction information (i.e., transactions exceeding $25,000 and less than $25,000). Upon written request of the GSA Contracting Officer, the ordering Contracting Officer, the Agency/Organization Program Coordinator (A/OPC), or the Internal Revenue Service with A/OPC knowledge and approval, the Contractor shall provide the requested information in an electronic format within 30 calendar days, unless otherwise specified at no additional cost to the Government. In addition, the Contractor shall provide online access to data for a minimum of 18 months after the transaction occurs.