

## STATEMENT OF WORK

for

### **Workout Advisory and Related Services**

FTI CONSULTING, INC (“**Supplier**”), MS FACILITIES LLC, a Delaware limited liability company (the “**Company**”), the Federal Reserve Bank of Boston (the “**Bank**”), as managing member of the Company (the “**Managing Member**”) enter into this Statement of Work (“**SOW**”) for Services pursuant to the Professional Services Agreement between the parties having an Effective Date of March 1, 2021, including all amendments thereto, (the “**Agreement**”). This SOW is entered into pursuant to and governed by the terms of the Agreement, which is incorporated herein by reference. All Services provided hereunder by the Supplier shall conform to the Service Standard. This SOW shall be effective for the period of time defined below.

### **Loan Tiers**

Loan participations are tiered by original loan balance value as follows (the “**Loan Tiers**”):

- Tier 1a - Amounts up to and including \$2,000,000
- Tier 1b - Amounts greater than \$2,000,000 to \$10,000,000
- Tier 2 - Amounts greater than \$10,000,000 to \$25,000,000
- Tier 3 - Amounts greater than \$25,000,000

### **Description of Services:**

1. Workout Application<sup>1</sup> Set-Up. The Supplier shall provide the following via resources located in the United States
  - a. Provide a controlled, efficient and cost-effective technology solution, which meets all requirements defined in Attachment G of the Agreement which shall facilitate workout loan analytics and the workout loan management program.
  - b. *Integration.* The Workout Application shall integrate with other technology platforms, which may be owned and managed by third parties, used in relation to the MSLP. The Supplier shall cooperate with such third parties to the extent necessary to effectuate integration.
  - c. *Configuration.*
    - i. The configuration of the Workout Application shall include data and document transmission functionality via API integration with Guidehouse’s Salesforce platform and communications functions for the Eligible Lender, SPV and third parties.
    - ii. The Supplier shall perform an initial penetration test of the Workout Application prior to go-live and provide the Company with a complete and detailed report of the results.

---

<sup>1</sup> As defined in Attachment G, Section 1.5 of the Agreement.

- iii. The Workout Application shall be specifically configured to usher a loan through all phases of a workout from ingestion of required documentation, through financial analysis, to recommendation and approval.

d. *Additional Application Performance Standards.*

- i. *Online Services Availability.* Supplier shall use best efforts to make Online Services accessible and operational twenty-four (24) hours a day, seven (7) days a week throughout the term of the statement of work. Company understands from time to time that Online Services may be unavailable or inaccessible; however, Supplier shall meet or exceed a Monthly Availability of at least 99.5%. Supplier shall use best efforts to minimize any disruption, inaccessibility and/or inoperability of the Online Services during periods of Scheduled Downtime and Unscheduled Downtime
- ii. *Unscheduled Downtime Notification.* Supplier shall use best efforts to provide notice to Company within one (1) hour of an occurrence of Unscheduled Downtime that is anticipated to continue for more than one (1) hour.
- iii. *System Response Time.* Supplier shall use best efforts to ensure a reasonable System Response Time to execute a transaction for not less than 95% of all Online Services transactions during each month as measured by response time to execute a transaction.
- iv. *Scheduled Downtime.* Supplier shall use best efforts to schedule Scheduled Downtime for routine maintenance, systems repair, and systems upgrades each week from **8:00 PM Saturday to 8:00 AM Sunday Central Time**. Scheduled Downtime shall not exceed eight (8) hours per month unless specifically approved by Company. Supplier shall notify Company of planned Scheduled Downtime as mutually agreed by the parties, but in no event less than 72 hours in advance. Supplier reserves the right to change Scheduled Downtime period with 72 hour advance prior notice to Company; provided, however, Supplier shall make every effort to schedule maintenance, systems repairs and systems upgrades during low utilization periods (typically nights, weekends and holiday periods) of the Online Services.

2. Workout Advisory Services and Workout Application Support Services: The Supplier shall provide workout advisory services listed below related to loan participations purchased by the Company. Such services shall include, but are not limited to the following:

a. *Workout Loans.*

- i. Assist Company in preparing policies and procedures for the oversight of the workout portfolio, including defining metrics and triggers that will require loans, or segments of the workout portfolio, to be managed as workout loans with heightened oversight (“**Workout Loan**”).
- ii. The Company may also determine a loan is a Workout Loan that does not meet the identified metrics and triggers in its discretion.

- iii. Develop a scorecard for Workout Loans to assess credit quality, underwriting quality and servicing effectiveness standards on loan administration conducted by an Eligible Lender (“EL”) (“**Scorecard**”).
  - iv. Use the Scorecard to assess the credit quality, underwriting quality and servicing effectiveness standards on loan administration conducted by an EL and provide such assessment to the Company.
  - v. Design workflow and decisioning rules for ELs and the management of their Workout Loans (“**Active Management**”). This will include, but is not limited to, project management, negotiation and structuring approaches for all types of workout scenarios, either out of court or in-court restructuring, liquidation or bankruptcy.
- b. *Collection Strategies.* Work with Company to develop cost efficient collection strategies for segments of the loan portfolios seeking to maximize recoveries and minimizing costs. Such strategies may include a collection automation strategy for portions of the workout portfolio, a loan sale strategy or other recovery strategies that conform to applicable laws and regulations and that are consistent with the overall policy objectives of the MSLP. The Company will provide further direction and clarifications as necessary on acceptable strategies.
- c. *Valuation Framework.* Establish a valuation framework, specific reserve assessment framework, and charge-off protocols for Workout Loans. Such frameworks should include discounted cash flow analysis, going concern and collateral liquidation valuations to support overall value and calculation of specific reserves or charge-offs on individual loans. Any valuation approach should comply with the required Company accounting standards. In addition, the frameworks should include a clear audit trail with supporting documentation.
- d. *Reserves and Charge-Offs.* Assist the Company in determining appropriate reserves and charge-offs for Workout Loans. Specific reserves and valuations shall be presented to the Company for review and approval. Additionally, final reserves shall be transmitted to the Company, Custodian, Administrator, and Credit Administrator.
- i. Supplier shall use commercially reasonable efforts to provide recommendations within 4 business days when information has been received, provided that volume of the request is distributed starting four weeks before the Credit Committee meeting for each quarter or Company communicates the timing of the volume bulk so the Supplier can plan staff resources to manage process. If unable to meet timeline due to unforeseeable high volume, the Supplier will notify the Company no later than the end of the third business day after receipt of the information.
  - ii. Supplier shall use commercially reasonable efforts to provide a summary report by 3 business days before the Credit Committee meeting for each quarter.
- e. *Disposition Analysis:*
- i. Assist the Company with hold/sell analysis for Workout Loans as requested.

- ii. Provide recommendations for the disposition of assets within the workout portfolio.

f. *Reporting.*

- i. Work with Custodian, Administrator, and Credit Administrator, as needed to prepare portfolio reporting and to collect and/or develop reporting required from the EL and borrower.
- ii. Review reporting from EL(s) and provide ongoing assessment of EL(s) performance.
- iii. Assist the Company in developing reporting for Workout Loans, including content and frequency. Establish reporting cadence with credit-specific status updates, distressed credit trend analytics and macro insights on industry health.
- iv. Provide reports on the following activities in a standardized format and frequency:

<b>Report</b>	<b>Frequency</b>
Status of all Review Requests	Daily
Status of all Workout Loans in Active Management	Weekly
Report for use in tracking the loan loss rate	Monthly
Status of Loans	On request

For customize or ad-hoc reports, Supplier will use commercially reasonable efforts to provide the report in a timely manner.

g. *Communications Protocol.* In cooperation with the Credit Administrator and the Company:

- i. develop policies, procedures and controls for communicating with ELs and collecting agreed-upon documentation in support of assessments and negotiations with controlled, auditable approach to documentation tracking;
- ii. establish policies, procedures and controls for leading negotiations with ELs on distressed loans; and
- iii. communicate directly with an EL as defined by the communication protocols defined above.

h. *Risk Mitigation.* Provide guidance on approaches to mitigating portfolio risk.

i. *Workout Administrator Management Support*

- i. Assist the Company in preparing guidelines and procedures for Workout Administrators procuring other necessary third-party vendors, including but not limited to field examiners, and asset valuation advisor.
- ii. Workout Advisor will provide oversight of the Workout Administrator(s), including providing the Company with hiring and firing recommendations.
- iii. Review reporting from Workout Administrator(s) and provide quarterly ongoing assessments of Workout Administrator(s) performance.
- iv. Develop and propose a conflicts of interest framework and will be utilized with other Workout Administrators, as defined below.

- j. *Core Rights Act*. Provide Company with a preliminary review and assessment of Core Rights Act<sup>2</sup> applicability and amendment requests prior to final determination if the request meets the threshold for requiring Simple Loan Modification Services (Level 1 Services), as defined in section 4 below, or Active Loan Management (Level 2 Services) as defined in section 5 below.
- k. *Preliminary Assessment*. Supplier shall use commercially reasonable efforts to provide Company with its preliminary assessment if the request meets the threshold for requiring Level 1 Services or Level 2 Services within two business days of receipt of request from the Company. Notwithstanding the above, Supplier shall process all requests as promptly as commercially reasonable. For the avoidance of doubt, input from a legal advisor shall not be considered part of the preliminary assessment. If unable to meet timeline due to unforeseeable high volume, the Supplier will notify the Company no later 24 hours after receipt of the request from the Company.
- l. *Audit Response and Support*. The Supplier shall provide the following support in a timely manner:
  - i. Assist the Company in responding to the requests of the Company's and Bank's internal and external auditors, including Oversight Entities, as defined in the Agreement;
  - ii. Cooperate with Oversight Entities, the Company, and the Bank, in preparing for, and responding to requests for information; and
  - iii. Comply with all obligations of the Supplier defined in Section 18 of the Agreement.
- m. *Testimony*. The Supplier shall provide any testimony or disclosure as may be required under the requirements and restrictions of section 8.1 of the Agreement. For any testimony that is required or requested, Supplier shall be compensated at its standard hourly rates less 20% and reimbursed for its reasonable, documented, out-of-pocket expenses (including counsel fees) with respect thereto.
- n. *Testimony Support*. All support provided to the Company for testimony the Company is required to give is contemplated as part of the monthly retainer fee, but not to exceed 15 hours per each time the Company is requested to testify ("Testimony Support Services")
- o. *Meetings and Reporting*. The Supplier shall attend meetings and provide reporting as defined in any Statement of Work executed under the Agreement and as required by section 13 of the Agreement.
- p. *Workout Application<sup>3</sup> Ongoing Service and Support*. Supplier shall provide the following services via resources located in the United States:

---

<sup>2</sup> As defined in the Participation Agreement Under the Main Street Lending Program, Standard Terms and Conditions found [here](#).

<sup>3</sup> As defined in Attachment G, Section 1.5 of the Agreement.

- i. ongoing support for provided solutions, including additional development necessary to maintain optimal functionality of the Workout Application and all support defined in Attachment G of the Agreement.
  - ii. access to the Workout Application for up to fifty (50) defined users to the Workout Application. Users designated by the Company may be employees of the Bank or a third-party service provider of the Company or the Bank.
  - iii. Supplier's developers and Workout Application team will work alongside Supplier workout experts, the Company, and other key stakeholders to ensure all components of the Workout Application are appropriately documented, tracked, and audit ready.
  - iv. The Workout Application shall be configured to generate dashboards to respond to any ongoing and ad-hoc reporting requests, such configuration may be updated from time to time at the request of the Company.
- q. *Other Services as Requested.* Provide other workout advisory services as requested, including reviewing and making recommendations on existing Company policies and procedures.

**3. Third-Party Vendors.** Supplier will identify required third-party vendors (e.g., perform valuations, collections services, etc.) define requirement and selection criteria, and source and procure the parties in support of the Simple Loan Modification (Level 1) and Active Management (Level 2) and Workout Advisory services if requested by the Company ("Sourcing Plan"). The Company or the Bank, as Managing Member of the Company, shall review and approve any Sourcing Plan, including selection criteria. Such approval shall not be unreasonably withheld. Selection criteria shall include, at minimum, commercially reasonable pricing. All such third-party vendors will be subcontractors to FTI and FTI, will manage and retain full responsibility for the performance of such vendors, including monitoring their performance and handling invoices and payment, in compliance with the terms of the Agreement, including but not limited to ensuring that all third-party vendors will be located in the United States. Notwithstanding anything to the contrary in the Agreement, Third-party vendors shall be required to comply with the provisions defined in Attachment 1 to this Statement of Work.

- a. All such third-party vendors costs shall be charged to the Company as a pass-through, without mark-up. Supplier will provide invoices from the third-party vendors services being charged to the Bank.
- b. Supplier shall provide Company with agreed upon quarterly summary of 3<sup>rd</sup> party vendor spend within 10 working days of quarter end.
- c. Subject to agreement on format and scope of the third party scorecards, Supplier shall provide Company with quarterly scorecards defining the top 5 other third parties (i.e., liquidators, appraisers, field auditors, etc.) based on the amount of fees incurred within 10 working days of quarter end.

- d. Supplier shall use commercially reasonable efforts to ensure that 95% of third-party invoices submitted quarterly to Company for reimbursement meet the Company's invoicing requirements upon the initial submission.
- e. Supplier understands the third-party legal counsel be will sourced, procured, contracted and managed by the Company. Supplier will advise as requested in such procurements. Supplier shall cooperate and collaborate with these third-party legal counsels as required for the Workout Administration Services

4. Simple Loan Modification Requests (Level 1 Services).

- a. Simple Loan Modification Requests are requests for approval of an amendment or loan modification where the EL has already negotiated with the borrower and is presenting a completed workout proposal, with completed draft documentation requiring only an approval and signature from the Company, for one or more of the following types of actions:
  - i. Delay or postponement of any date scheduled for any payment of principal, interest, fees or other amounts payable for six (6) months or less from the original scheduled payment date, provided such delay or postponement does not include any permanent waiver or forgiveness of such amount and is not more than the second time that such a delay has been done;
  - ii. Reduction in the rate of interest or reduction in any fees payable;
  - iii. Waiver of any condition precedent to closing, effectiveness or funding under the Credit Agreement;
  - iv. Amendment to, modification of, waiver of or consent to any departure from any provision in any Credit Document relating to Borrower's certifications and covenants, including but not limited to financial covenants, covenants in Section 2 (CARES Act Borrower Eligibility Certifications and Covenants) or Section 3 (FRA and Regulation A For Borrower Eligibility Certifications) of the Borrower Certifications and Covenants; and
  - v. Amendment to, modification of, waiver of or consent to any departure from any provision in any Credit Document requiring the periodic financial reporting by Borrower or any other Obligor.
- b. For Simple Loan Modification Requests, the Supplier shall:
  - i. Review loan modification, and amendment or waiver requests ("**Request Reviews**") for completeness and assess appropriateness as it relates to Core Rights Act. Such review may include legal opinions and associated financial impacts and policy considerations.
  - ii. The level of review activity for each Review Request shall be determined by the Loan Tier and defined in the governance documentation to be developed under section 1(a)(i) of this SOW.
  - iii. For Level 1 Services, Supplier shall use commercially reasonable efforts to provide recommendation for at least 75% of loan modification in a single quarter requests within 2 business days, after the request has been confirmed it is a Core Rights Act and the Supplier has received sufficient information to process the request, provided that the matter does not need

additional advice from third party, including and not limited to legal counsel or the Company or need additional information from the EL or Borrower, which may cause delays. If the matter requires extended time for review, Supplier will notify the Company.

- iv. Provide recommendations in a standardized form to the Company to facilitate timely voting and responses to Review Requests and notices.

5. Active Management (Level 2 Services). Designation of any participation as a Level 2 service is subject to the review and approval by the Company. Active Management may include requests by the EL for consultation with regard to an actual or potential default or workout strategies (“Consultation”) or a formal request by the EL for approval of a specific proposed restructuring or loan modification to be considered for approval by the Company for one or more of actions listed below (“Level 2 Services Event”). The below list is not exhaustive.

- i. Delay or postponement of any date scheduled for any payment of principal, interest, fees or other amounts payable for greater than six (6) months from the original scheduled payment date or is the second time that such a delay has been requested;
- ii. Any extension, increase or reinstatement of any commitment with respect to the Transferred Rights or Assumed Obligations;
- iii. Any reduction in the principal in respect of the Transferred Rights or Assumed Obligations, including, without limitation, any Loan Forgiveness;
- iv. Any release of all or substantially all of the collateral provided for the Transferred Rights or Assumed Obligations in any transaction or series of transactions or all or substantially all of the value of the Guaranties in respect of the Transferred Rights or Assumed Obligations;
- v. The express subordination of (A) the Loans or (B) any Encumbrance in or over all or substantially all of the Loan Collateral that has been, or is purported to have been, granted (or otherwise created) to or for the benefit of the Lenders under the Credit Documents;
- vi. The exercise, or failure to exercise, of any rights or remedies with respect to any of the Loan Collateral at any time that Seller or any Commonly Controlled Affiliate of Seller, or any of their respective agents or representatives, is exercising rights or remedies with respect to any collateral securing, or purporting to secure, any indebtedness owed by Borrower to Seller or any Commonly Controlled Affiliate of Seller the default under which has resulted in a Seller Debt Cross-Acceleration;
- vii. Any change to any lender voting approval level under or pursuant to any Credit Document with respect to any of the foregoing;
- viii. Any change of the pro rata sharing provisions or application of proceeds provisions in the Credit Documents affecting the Transferred Rights or Assumed Obligations;
- ix. Any greater restriction on the ability of, or any additional consent necessary for, any Lender to assign, participate or pledge its rights or obligations under any Credit Document;
- x. An adverse effect on the Transferred Rights that would be disproportionate to the effect on any other class of obligations under a Credit Document;



- xi. Any amendment to, modification of, waiver of or consent to any departure with respect to any provision in any Credit Document that provides a default or event of default upon the acceleration of any other indebtedness owed by Borrower to Seller or a Commonly Controlled Affiliate of Seller (any such default or event of default, a “Seller Debt Cross-Acceleration”); and
- xii. The declaration, or failure to declare, any obligations of Borrower due and payable upon the occurrence and during the continuance of a Seller Debt Cross-Acceleration.

6. As part of the Active Management Services, Supplier shall:

- a. Oversee workout activity by ELs, including, but not limited to the assessment of legal opinions and associated financial impacts and policy considerations.
- b. Provide advice and direction to the Company regarding the workout plan being presented and deployed by the EL.
- c. Provide assessment and implementation of the workout plan, including specific reserve and charge-off recommendations, provided to the Company by an EL, including any applicable analytics for the Workout Loan.
- d. In the event of a specific request for the Company’s approval of a loan modification request, Supplier shall use commercially reasonable efforts to provide recommendation on at least 75% of loan modification requests in a single quarter, within nine (9) business days, after the request has been confirmed as a Core Rights Act and the Supplier has received sufficient information to process the request. If the matter requires additional time for review, Supplier will notify the Company within five (5) business days after the request has been confirmed as a Core Rights Act.
- e. In the event of a request for Consultation, Supplier will engage with the EL to develop a restructuring or loan modification plan that the Supplier is willing to recommend to the Company within nine (9) business days. The recommendation will be provided to the Company no more than nine (9) business days from the date of the EL’s request. Requests of this type will be aggregated with request from (d) above for purposes of determining the 75% threshold.

**Service Term:**

This SOW shall be effective commencing on March 1, 2021 and shall end on February 28, 2022, unless earlier terminated pursuant to the Agreement. The parties may renew this SOW for like terms by mutual written agreement no later than February 28, 2022. The Company shall provide the Supplier with thirty (30) days prior written notice if this Statement of Work will not be renewed. In no event shall any fees defined in this SOW increase by more than the Consumer Price Index, as defined by the Bureau of Labor Statistics for the Boston-Cambridge-Newton region.

**Fees and Payment Terms:**

<b>Workout Application Set-Up</b>	
	<b>One-Time Fee</b>
Set-Up Fee	\$1,600,000

<b>Workout Advisory and Ongoing Workout Application Support Services</b>	
<b>Estimated Hours</b>	<b>Monthly Retainer Fee</b>
993	\$480,000

Fees for work not contemplated by the Monthly Retainer Fee in excess of fifteen (15) hours per request, including but not limited to Disposition Analysis work, Testimony Support Services and other ad hoc projects, shall be agreed to between the Parties in a separate statement of work and shall be charged time and material by the Supplier at the then-current time multiplied by standard rates hourly rates less 20% . The material will be billed at cost with no mark-up or discount.

<b>Simple Loan Modification (Level 1)</b>	
<b>Loan Tier</b>	<b>Pricing<sup>4</sup> - Basis Points Per Event</b>
Tier 1a (Up to and including \$2,000,000)	15.00
Tier 1b (Greater than \$2,000,000 and to \$10,000,000)	5.00
Tier 2 (Greater than \$10,000,000 to \$25,000,000)	4.00
Tier 3 (Greater than \$25,000,000)	3.00

**Invoice Terms:** Fees for Simple Loan Modifications shall be invoiced in the month following the submission of the loan modification.

<b>Active Management (Level 2)</b>
------------------------------------

<sup>4</sup> Basis Points multiplied by the Original MSLP Total Loan amount of credit undergoing Level 1 services. All per-event Basis Points fee will be assessed on the Original MSLP undergoing Level 1 services. For clarity, this is defined as the total amount of the loan as originated under the MSLP and not the participation amount or current balance.

<b>Loan Tier</b>	<b>Pricing<sup>5</sup> - Basis Points Per Event</b>
Tier 1a (Up to and including \$2,000,000)	170.00
Tier 1b (Greater than \$2,000,000 to \$10,000,000)	120.00
Tier 2 (Greater than \$10,000,000 to \$25,000,000)	70.00
Tier 3 (Greater than \$25,000,000)	50.00

**Invoice Terms:** Fees for Active Management (Level 2) shall be invoiced per event in two parts. The first half of the fee shall be invoiced in the month following the loan being approved for Level 2 Services by the Company, triggered by either a Consultation or a formal request for approval of a specific proposed restructuring or loan modification. The second half of the fee shall be invoiced following final resolution and closeout, whether triggered by a loan leaving Workout Loan status, including but not limited to the loan being upgraded to a pass rating, execution of the final legal documents required by a mutually agreed upon workout plan or completion of a restructuring transaction, liquidation of the borrower and/or all collateral, or exit from a bankruptcy with the expectation each event could last from 3 to 18 months.

Additional Scenarios

- In the event a loan is sold during Level 2, the second half of the payment for Level 2 will not be due for that Workout Loan. The Supplier shall invoice the Company for any disposition work conducted after a determination that the loan will be sold at the current standard rates, less 20%, plus materials at cost and as defined in a mutually agreed separate statement of work.
- In the event of an Elevation during Level 2 services to Level 3, where the first payment for Level 2 services is made, applicable fees for Level 3 services will be invoiced. No second payment for Level 2 services will be due or payable.
- In the event that a loan is successfully restructured and subsequently requires Level 2 or Level 3 services, all fees for such services will apply.
- Other scenarios that arise relating to Level 2 and Level 3 Services which are not defined above shall be mutually agreed between the Supplier and the Company in writing.

<b>Specific Reserve Assessment Fees</b>
---

---

<sup>5</sup>Basis Points multiplied by the Original MSLP Total Loan amount of credit undergoing Level 2 services. All per-event Basis Points fees will be assessed on the Original MSLP Total Loan amount of credit undergoing Level 2 services. For clarity, this is defined as the total amount of the loan as originated under the MSLP and not the participation amount or current balance.

Loan Amount	Pricing <sup>6</sup> - Basis Points Per Event
\$15,000,000 or greater	0.80

**Invoice Term:** Fees for Specific Reserve Assessments shall be invoiced in the month following completion of the quarterly specific reserve assessment. For the avoidance of doubt, fees will only be charged on loans requiring an assessment in a given quarter. In the event that a loan is in the specific reserve process but there has not been a material update to the documentation or updated financials are not provided, a review will not be required and fees will not be charged to roll forward the prior quarter's analysis.

Each level of service must be completed prior to work commencing on a new level of service. For the avoidance of doubt, Level 1 and Level 2 Services are billable only under this Statement of Work for Advisory and Related Services. Level 3 Services are billable only under the Statement of Work for Workout Administration Services.

**Monthly Reporting to Support Invoicing.** FTI will provide monthly reporting on the numbers of loans and status (initiated, in-process, completed and sold), the start and end date (if applicable) of each loan, the respective individual loan sizes and applicable basis point fees in each Tier and each Level to the Company for review. For Specific Reserve assessment, FTI will provide a list of loans reviewed with original loan size and applicable basis point fees. For any work completed under time and materials, FTI will provide monthly reporting on people, hours and activity summary.

**Travel:** All travel expenses must be pre-approved by the Bank and incurred and reported in conformance with the Bank's Non-Employee Travel Guidelines which will be provided to the Supplier on request.

### **Program Managers**

The following are the Supplier's contacts for the Services defined in this SOW:

*[Signature Page to Follow]*

---

<sup>6</sup> Basis Points multiplied by the aggregate Original MSLP Total Loan amount reviewed under this assessment. Note: Per event pricing for specific reserve assessment is limited to loans initially sized \$15,000,000 or greater. Basis Points pricing is subject to change if this threshold is reduced or eliminated.

By signing in the signature blocks below, Bank, Company and Supplier agree to the terms of this SOW pursuant to the Agreement.

**AGREED:**

**FTI CONSULTING, INC.**

By:

Name:

Title: Co-Leader Corporate Finance

**AGREED:**

**MS FACILITIES LLC**

By: Federal Reserve Bank of Boston as its  
Managing Member

By:

Name:

Title: Executive Vice President

**AGREED:**

**FEDERAL RESERVE BANK OF  
BOSTON**

By:

Na

Title: First Vice President and Chief  
Operating Officer

## Attachment 1

### Subcontract Minimum Required Terms

This Attachment 1 defines I) the minimum required terms that must be included in all Subcontractor agreements the Supplier enters into to perform the Services defined in a Statement of Work, and II) requirements that will be included if applicable to the specific services to be provided, as defined below.

For the purposes of this attachment, the following definitions apply:

“Subcontractor” refers to a subcontractor of the Supplier.

“Subcontractor Personnel” means all employees, personnel, agents, representatives, and subcontractors, any other persons directly or indirectly employed by a subcontractor of the Subcontractor, and any other persons who perform work associated with the Services provided to Supplier by the Subcontractor under the Statement of Work.

“Bank Affiliate” means any entity in the Federal Reserve System, including, but not limited to, each of the Federal Reserve Banks and the Board of Governors.

#### I. Minimum Required Terms

1. Third Party Beneficiary. The Supplier shall name Bank as a third-party beneficiary under each of the Supplier’s agreement with any Subcontractor required to perform the services under a Statement of Work.

2. Performance. The Subcontractor will perform the Services (1) in accordance with the generally recognized standards of the Supplier’s profession, (2) with a level of care, technical skill, diligence, frequency, volume, amount and detail commensurate with the requirements of the Service, conforming to any specified Statement of Work and at least equal to the standards the Supplier applies to services performed for other comparable accounts and (3) in a manner consistent with all applicable legal requirements and (C) any other prevailing standards for such Service in the relevant industry (the foregoing clauses (1) through (3), the “Service Standard”).

3. Service Location. For the avoidance of doubt, Services will be provided by Supplier Personnel, as defined below, located in the United States. All Company information that is stored, processed, or transmitted by the Subcontractor shall remain stored, processed, or transmitted in the United States.

#### 4. Confidentiality, Security and Controls

4.4 *General*. “Confidential Information” means any information disclosed to any Subcontractor Personnel, in whatever form obtained from or through the Bank (including information from or about any Bank Affiliate) or developed by or otherwise obtained by the Subcontractor in connection with the performance of this Agreement, including, but not limited to, all information relating to the Company or the Bank’s supervisory, regulatory, research, development, and business activities, security, data files, personnel information, and computer programs. The Subcontractor shall hold, and shall ensure that all Subcontractor Personnel hold, all such information confidential and shall not disclose to any person, firm, corporation, or other entity, nor use for its own business or benefit, any Confidential Information obtained or generated by it during the term of this Agreement. The Subcontractor shall take all reasonable measures to recover any Confidential Information wrongfully disclosed.

4.5 The Bank, in addition to any other remedy available to it by law, shall be entitled to injunctive relief to enforce this confidentiality provision.

4.6 If the Subcontractor is compelled to testify against the Bank by subpoena or court order, or if the Subcontractor is required to disclose Confidential Information pursuant to applicable law or is required to provide Confidential Information to a regulatory agency, it shall give prompt written notice to the Bank, and afford the Bank the opportunity to review, in advance, any information being disclosed. In the event Subcontractor and/or any of its employees are required to testify or provide evidence at or in connection with any judicial or administrative proceeding relating to this Agreement to which Subcontractor is not a party, the Company will compensate Subcontractor at its regular hourly rates and reimburse Subcontractor for reasonable, documented, out-of-pocket expenses (including counsel fees) with respect thereto. Nothing in this Agreement shall restrict the Subcontractor's use of information that is or becomes: (i) publicly available through no breach of this Agreement; (ii) previously known to the Subcontractor without obligation of confidence; or (iii) acquired by the Subcontractor from a third party which is not under an obligation of confidence with respect to such information.

4.7 As requested by the Bank, the Subcontractor, and all Subcontractor Personnel, will terminate all electronic and physical means of accessing the Bank's Confidential Information, and upon the Bank's request, return or securely destroy, at the Bank's option, and certify such destruction in writing to the Bank, all material in any medium that contains, refers to, or relates to Confidential Information, including all archived and back-up copies. The Subcontractor will return all Confidential Information in the possession of any Subcontractor Personnel to the Bank within 60 days after Agreement expiration or termination, regardless of whether or not the Bank has requested the return of the Confidential Information, and unless the Bank requests destruction of the Confidential Information. Further, except as set forth in this Agreement, Subcontractor will not acquire any right in or assert any lien against the Bank's Confidential Information, and/or refuse to promptly return, provide a copy of, or destroy such Confidential Information upon the request of the Bank.

4.8 *Delivery or Destruction Infeasible.* If the Subcontractor believes that the delivery or destruction of any Confidential Information is not feasible (including Confidential Information that is retained on secure backup media in accordance with standard backup procedures in a manner that makes it impractical for the Subcontractor to delete the Confidential Information), or if the Subcontractor is required by applicable law, accounting rules, or other professional rules to retain a copy of any Confidential Information for some period, the Subcontractor may retain a copy of such Confidential Information subject to the restrictions of this Section [TBD] until the Confidential Information becomes public or otherwise ceases to be Confidential Information as defined in Section [TBD], or is returned to the Bank.

## 5. Conflict of Interests

5.4 *Subcontractor Objectivity.* A conflict of interest exists for Subcontractor when other business relationships or financial interest of Subcontractor or Subcontractor's Affiliates or personal or business relationships, activities, and financial interests of those of Subcontractor officers or employees who are assigned to manage or perform the services under the Agreement could knowingly impair (a) Subcontractor's objectivity or impartiality in performing the Services or (b) the quality of the Services. It is Subcontractor's policy that all inherent and actual conflicts of interest be identified, evaluated, and either managed or avoided, as appropriate. Subcontractor warrants to the Company that no conflict of interest presently exists. If circumstances arise during

the term of the Agreement that create or could create a conflict of interest, subject to its obligations of confidentiality, Subcontractor shall notify the Bank promptly and take such steps as the Bank may request to avoid, neutralize, or mitigate the conflict of interest. If the Bank determines that the conflict of interest cannot be avoided, neutralized, or mitigated in a manner satisfactory to the Bank, the Bank may terminate the Agreement upon notice to Subcontractor.

5.5 *Misuse of Information for Private Gain.* Neither Subcontractor nor any of its Subcontractor Personnel may use any Confidential Information except to fulfill the purposes of the Agreement and as expressly permitted in the Agreement. This restriction prohibits, without limitation, the knowing use of any Confidential Information for the benefit of Subcontractor or any of its Affiliates or their respective directors, officers, or employees (beyond the benefit of the consideration to be received by Subcontractor under the Agreement), for the benefit of any other Subcontractor client, or to inform any financial transaction, render any advice or recommendation, or attempt to influence any market or transaction for the benefit of any individual or entity.

5.6 *Vendor Bias.* Subcontractor shall not recommend to the Company or Bank in connection with Subcontractor's performance of services any products or services of an individual or entity (including Affiliates of Subcontractor) from which Subcontractor may receive a financial incentive based on (a) Subcontractor's recommendation of the product or service to the Bank or Company or (b) the Bank's purchase of the product or service, unless, in each case, Subcontractor first discloses in writing to the Bank the nature of the relationship and the specific terms of any financial incentive Subcontractor may receive.

5.7 Subject to its obligations of confidentiality, Subcontractor shall disclose potential conflicts of interest to the Bank as they arise and, at the request of the Bank will cooperate with the Company and the Bank to mitigate or avoid the conflict or if the conflict cannot be adequately mitigated or avoided, in the Bank's sole discretion, recuse itself from providing the services.

5.8 Subcontractor's conflict of interest records shall specifically describe the steps Subcontractor will take to mitigate the conflict that could arise from an Affiliate of Subcontractor participating or seeking to participate as sponsor of any participant in the Main Street Facilities while Subcontractor is providing services under this Agreement.

5.9 *Conflict Reporting and Records.* Employees of Subcontractor shall be required to report promptly any breach or suspected breach of these conflicts requirements to FTI. Subcontractor shall also conduct periodic reviews of its conflicts policy and/or associated compliance procedures.

5.10 *Insider Trading Restrictions.* The information barrier procedures provided under this Agreement shall contain investment restrictions and monitoring measures as deemed necessary and appropriate by Subcontractor to prevent "behind the wall" individuals from knowingly trading in the securities of originating institutions or borrowers under the Main Street Facilities or otherwise trading on inside information gathered through the course of providing services to the Bank and Company. This procedure shall be provided to the Bank for review upon request.

5 Compliance with Law. The Subcontractor and all Subcontractor Personnel and their respective Subcontractors shall at all times comply with all applicable federal, state, and local laws, codes, regulations, ordinances, and rules, in performing the Services, including but not limited to, consumer privacy laws, OSHA (federal and state) and other worker-protection requirements and environmental protections. Subcontractor shall maintain during the term of this



Agreement any authorization, license, and permit as may be required by any such law or regulation to perform the Service. The Subcontractor shall notify the Bank immediately in writing in the event or likelihood of termination of any such authorization, license, or permit.

- 6 Equal Opportunity. By entering into this Agreement, the Subcontractor confirms its commitment to equal opportunity in employment and contracting. To implement this commitment, the Subcontractor shall, to the maximum extent possible consistent with applicable law, provide for the fair inclusion of minorities and women in its workforce.
- 7 Ethics Statement and Gratuities. The Subcontractor shall perform services with honesty and integrity using its best skill and judgment and in the most expeditious and economic manner consistent with the Bank's policies, which can be found on the [Doing Business With Us](#) section of the Bank's website. Also, the Subcontractor, its employees, agents, or subcontractors shall not extend any gratuity or special favor to the Bank's employees.
- 8 Publicity. Neither the Subcontractor nor any of the agents, affiliates, or parties under its respective control shall use the Bank or the Company's name, or the name of any Federal Reserve System entity, or any adaptation or variation of such name in any advertising or promotional material or other publication, or otherwise publicize or communicate the Subcontractor's relationship with the Bank or the Company without the Bank and the Company's prior written consent.

## **II. Additional Terms to be Incorporated into Subcontracts as Applicable**

In addition to the minimum required terms defined above, the Supplier shall include the following terms which are applicable to the Services provided by the Subcontractor:

1. To the extent the Subcontractor has access to loan level information and information systems, the terms defined in Attachment 1-A.
2. To the extent the Subcontractor has access to SPV information and information systems, the terms defined in Attachment 1-B.
3. To the extent the Subcontractor has access to the Bank's information and information systems, the terms defined in Attachment 1-C.
4. To the extent the Subcontractor has access to Reserve Bank PII elements which are defined as Low or Very Low PII Element, as defined in Attachment 1-D, the terms defined in Attachment 1-D. To the extent the Subcontractor has access to Reserve Bank PII elements which are defined as Moderate PII Elements, as defined in Attachment 1-E, the terms defined in Attachment 1-E.
5. To the extent the Subcontractor has access to Reserve Bank PII elements which are defined as High PII Elements, as defined in Attachment 1-F, the terms defined in Attachment 1-F.

## ATTACHMENT 1-A

### Loan Level Information Security Requirements

This Attachment shall be included in all subcontracts for services that require access to the information regarding loans, but not including information regarding the portfolio or governance and without access to the Bank's premises, systems and/or network. For purposes of this Attachment, all references to the "Bank" include any Bank Affiliate, or other entity engaged or designated by the Bank.

1. *Access Agreements.* Any Subcontractor Personnel requiring access to the Bank's information or information systems must agree to appropriate access agreements (e.g., nondisclosure agreements, conflicts of interest agreements, and access agreements) as provided or required by the Bank before access is granted and may be required to acknowledge, by written or electronic signature, their responsibilities and expected behavior with respect to information and information system usage.
2. *Personal Devices.* Subcontractor Personnel may not connect personal devices (e.g., USB Flash Memory drives, MP3 players, external hand devices, cell phones, etc.) to any computer, network, or electronic messaging resources of the Bank without authorization from the appropriate information asset owner.
3. *Authentication Credential Requirements.* All Subcontractor Personnel must have proper authorization and authentication credentials to access any computer, network, or electronic messaging resources of the Bank. Subcontractor Personnel are responsible for securely managing all authentication credentials in accordance with the Bank's standards and all authentication credentials must not be shared with others. Subcontractor Personnel may not attempt to circumvent approved authentication processes and procedures or access controls.
4. Encryption of External Media Devices. All Subcontractor Personnel utilizing portable media devices which contain data, proprietary information, Confidential Information, or authentication information of the Bank must ensure such devices are encrypted according to the Bank's standards (e.g., USB Flash Memory drives).
  - (i) Reporting Security Breaches. As used herein, "Incident" means any event that jeopardizes the confidentiality, integrity, or availability of Confidential Information. Incidents include an actual or suspected loss, theft, misuse, unauthorized disclosure or acquisition of, or unauthorized access to Confidential Information, regardless of whether it creates a likelihood of harm. Any security Incident or suspicious activity that involves data, proprietary information, Confidential Information, access, or authentication information of the Bank, or the loss or destruction of the Bank's property must be promptly ( ) reported to the Bank (e.g., if a laptop containing the Bank's information is stolen, the theft must be promptly reported to the appropriate authority).
  - (ii) Remote Access. Subcontractor Personnel will not share their remote access configuration.
5. *Termination of Access.* Any data or system information captured, viewed, saved, or disseminated in any way, is proprietary information of the Bank and must be returned to the Bank upon termination or expiration of access. Upon completion of the Services or expiration

or termination of this Agreement, whichever occurs first, the Subcontractor will ensure that all property and data relating to the Services are returned to FTI Consulting or destroyed.

6. *Breach Notification.* The Subcontractor will take all commercially reasonable measures to secure and prevent unauthorized entry, modification, or access to any systems on which the Bank information is transmitted or stored. The Subcontractor will promptly ( ) notify the Bank at of any breaches of security or unauthorized access to the Subcontractor's systems used to provide Service. The Subcontractor will use diligent efforts to remedy such breach of security or unauthorized access in a timely manner. In the event of any breach of this Attachment, the Subcontractor shall notify the Bank promptly ( ) upon becoming aware thereof.
7. *Remedies.* The Subcontractor understands that failure to carry out the requirements of this Agreement may result in the exercise of all remedies at law or equity available to the Bank.

## ATTACHMENT 1-B

### SPV Information Security Requirements

This Attachment shall be included in all subcontracts for services that require access to the information of the Company, including but not limited to portfolio information or governance documentation, and without access to the Bank's premises, systems and/or network. For purposes of this Attachment, all references to the "Bank" include any Bank Affiliate, or other entity engaged or designated by the Bank.

1. *Access Agreements.* Any Subcontractor Personnel requiring access to the Bank's information or information systems must agree to appropriate access agreements (e.g., nondisclosure agreements, conflicts of interest agreements, and access agreements) as provided or required by the Bank before access is granted and may be required to acknowledge, by written or electronic signature, their responsibilities and expected behavior with respect to information and information system usage.
2. *Inspection Rights.* Except as prohibited by applicable law, the Bank will be afforded access to the technical capabilities, operations, documentation, records, and data bases of all Subcontractor Personnel under this Agreement for the purpose of carrying out a program of inspection to ensure continued efficacy and efficiency of safeguards against threats and hazards to data information security, integrity, and confidentiality.
3. *Personal Devices.* Subcontractor Personnel may not connect personal devices (e.g., USB Flash Memory drives, MP3 players, external hand devices, cell phones, etc.) to any computer, network, or electronic messaging resources of the Bank without authorization from the appropriate information asset owner.
4. *Authentication Credential Requirements.* All Subcontractor Personnel must have proper authorization and authentication credentials to access any computer, network, or electronic messaging resources of the Bank. Subcontractor Personnel are responsible for securely managing all authentication credentials in accordance with the Bank's standards and all authentication credentials must not be shared with others. Subcontractor Personnel may not attempt to circumvent approved authentication processes and procedures or access controls.
5. Encryption of External Media Devices. All Subcontractor Personnel utilizing portable media devices which contain data, proprietary information, Confidential Information, or authentication information of the Bank must ensure such devices are encrypted according to the Bank's standards (e.g., USB Flash Memory drives).
  - (i) Reporting Security Breaches. As used herein, "Incident" means any event that jeopardizes the confidentiality, integrity, or availability of Confidential Information. Incidents include an actual or suspected loss, theft, misuse, unauthorized disclosure or acquisition of, or unauthorized access to Confidential Information, regardless of whether it creates a likelihood of harm. Any security Incident or suspicious activity that involves data, proprietary information, Confidential Information, access, or authentication information of the Bank, or the loss or destruction of the Bank's property must be promptly ( ) reported to the Bank (e.g., if a laptop containing the Bank's information is stolen, the theft must be promptly reported to the appropriate authority).

(ii) Remote Access. Subcontractor Personnel will not share their remote access configuration.

6. *Termination of Access*. Any data or system information captured, viewed, saved, or disseminated in any way, is proprietary information of the Bank and must be returned to the Bank upon termination or expiration of access. Upon completion of the Services or expiration or termination of this Agreement, whichever occurs first, the Subcontractor will ensure that all Subcontractor Personnel terminate promptly all electronic and physical means of gaining access to the Bank's computer systems, including but not limited to, maintenance accounts and information security bypasses ("Access Privileges"). The Subcontractor will also ensure that all Subcontractor Personnel return all property and data of the Bank. At that time, the Subcontractor will provide the Bank with a list of all Subcontractor Personnel with Access Privileges to ensure Subcontractor's compliance with this Attachment.
  
7. *Breach Notification*. The Subcontractor will take all commercially reasonable measures to secure and prevent unauthorized entry, modification, or access to any systems on which the Bank information is transmitted or stored. The Subcontractor will promptly ( ) notify the Bank at of any breaches of security or unauthorized access to the Subcontractor's systems used to provide Service. The Subcontractor will use diligent efforts to remedy such breach of security or unauthorized access in a timely manner. In the event of any breach of this Attachment, the Subcontractor shall notify the Bank promptly ( ) upon becoming aware thereof.
  
8. *Remedies*. The Subcontractor understands that failure to carry out the requirements of this Agreement may result in the exercise of all remedies at law or equity available to the Bank.

## ATTACHMENT 1-C

### Bank Information Security Requirements

This Attachment shall be included in all subcontracts for services that require access to the Bank's premises, systems and/or networks. For purposes of this Attachment, all references to the "Bank" include any Bank Affiliate, or other entity engaged or designated by the Bank.

1. *General.* In performing the Services on the Bank's premises, all Supplier Personnel will comply with all of the Bank's information security policies, procedures, and requirements made available to the Supplier. Access to the Bank's information assets and computer resources and devices by any Supplier Personnel may only be implemented by specific approval from the Bank.
2. *Access Agreements.* Any Supplier Personnel requiring access to the Bank's information or information systems must agree to appropriate access agreements (e.g., nondisclosure agreements, conflicts of interest agreements, and access agreements) as provided or required by the Bank before access is granted and may be required to acknowledge, by written or electronic signature, their responsibilities and expected behavior with respect to information and information system usage.
3. *Access Monitoring.* Except as prohibited by law, the Bank may enter, search, and/or monitor at its discretion all computer and network equipment and any other computer or communications device provided by the Bank, including devices owned by any affiliate or other designee of Bank that are used to perform the Services pursuant to this Agreement with authorized or unauthorized access to any such resources. The Bank may also monitor the activities of any other computing device while that device is accessing the Bank's computers or network. Notwithstanding the foregoing, if the Bank discovers malicious activity or has reasonable belief that the Supplier's equipment was used to compromise the Bank's network or computers, such equipment will be immediately disconnected from the Bank's network or systems, and the Supplier will cooperate with the Bank, in a commercially reasonable way, to investigate such equipment. All Supplier Personnel, whether authorized or unauthorized, consent to the monitoring of their use of such resources and to the Bank's access to and disclosure of any voice communications or data stored on such equipment. Further, no information, however classified, which is stored or transmitted using such equipment, will be considered private information of any employee or other person, except as required by law.
4. *Inspection Rights.* Except as prohibited by applicable law, the Bank will be afforded access to the technical capabilities, operations, documentation, records, and data bases of all Supplier Personnel under this Agreement for the purpose of carrying out a program of inspection to ensure continued efficacy and efficiency of safeguards against threats and hazards to data information security, integrity, and confidentiality.
5. *Personal Devices.* Supplier Personnel may not connect personal devices (e.g., USB Flash Memory drives, MP3 players, external hand devices, cell phones, etc.) to any computer, network, or electronic messaging resources of the Bank without authorization from the appropriate information asset owner.
6. *Authentication Credential Requirements.* All Supplier Personnel must have proper authorization and authentication credentials to access any computer, network, or electronic messaging resources of the Bank. Supplier Personnel are responsible for securely

managing all authentication credentials in accordance with the Bank's standards and all authentication credentials must not be shared with others. Supplier Personnel may not attempt to circumvent approved authentication processes and procedures or access controls.

7. *Integrity of Computing Resources and Devices.* All Supplier Personnel are responsible for ensuring the integrity of all computing resources and devices which connect to any of the Bank's resources and which must meet the Bank's standards (including remote access to any of the Bank's systems). All Supplier Personnel must leverage antivirus, personal firewalls, desktop encryption, and any other required security software, and run the latest security patches on all computing resources and devices. Hardware, software, authentication devices, and communication or messaging equipment must be used only for purposes approved by the Bank. All internet access software used with and through any of the Bank's networks must be approved by the Bank and must be configured according to the Bank's information security standards. All internet connections made from any of the Bank's networked computing resources or devices must be made through the Bank's firewalls. All Supplier Personnel will take all necessary precautions to minimize the risk of virus infection to the Bank's network and computer system.
  - a. Encryption of External Media Devices. All Supplier Personnel utilizing portable media devices which contain data, proprietary information, Confidential Information, or authentication information of the Bank must ensure such devices are encrypted according to the Bank's standards (e.g., USB Flash Memory drives).
  - b. Reporting Security Breaches. As used herein, "Incident" means any event that jeopardizes the confidentiality, integrity, or availability of Confidential Information. Incidents include an actual or suspected loss, theft, misuse, unauthorized disclosure or acquisition of, or unauthorized access to Confidential Information, regardless of whether it creates a likelihood of harm. Any security Incident or suspicious activity that involves data, proprietary information, Confidential Information, access, or authentication information of the Bank, or the loss or destruction of the Bank's property must be promptly ( ) reported to the Bank (e.g., if a laptop containing the Bank's information is stolen, the theft must be promptly reported to the appropriate authority).
  - c. Remote Access. Supplier Personnel will not share their remote access configuration.
8. *Email Filtering.* All Supplier Personnel will have approved email filtering software that limits SpamWare, malware, or other malicious code transmitted through email installed on all computing resources and devices used while providing the Services.
9. *Approved Software.* Only licensed software provided by the Bank and in-house developed code (including Supplier developed code approved by the Bank) shall be used on the Bank's system. No public domain, shareware, or bulletin board software shall be installed. All additional hardware and software packages proposed for use, including upgrades, must be approved in advance and in writing by the Bank.
10. *Termination of Access.* Any data or system information captured, viewed, saved, or disseminated in any way, is proprietary information of the Bank and must be returned to the

Bank upon termination or expiration of access. Upon completion of the Services or expiration or termination of this Agreement, whichever occurs first, the Supplier will ensure that all Supplier Personnel terminate promptly all electronic and physical means of gaining access to the Bank's computer systems, including but not limited to, maintenance accounts and information security bypasses ("Access Privileges"). The Supplier will also ensure that all Supplier Personnel return all property and data of the Bank. At that time, the Supplier will provide the Bank with a list of all Supplier Personnel with Access Privileges to ensure Supplier's compliance with this Attachment.

11. *Reporting.* The Supplier shall deliver to the Bank written evidence of compliance with SSAE-18 documented in a SOC 2, Type II Audit Report, or other form of report acceptable to the Bank, on a biannual basis or upon the Bank's request. The Supplier shall also provide ConMon pen test results and vulnerability assessments, and an independent third party assessment of the Supplier's privacy program on at least an annual basis; provided that after the first annual report, a summary of such pen test results and vulnerability assessments may be provided.
12. *Breach Notification.* The Supplier will take all commercially reasonable measures to secure and prevent unauthorized entry, modification, or access to any systems on which the Bank information is transmitted or stored. The Supplier will promptly (b ) notify the Bank at of any breaches of security or unauthorized access to the Supplier's systems used to provide Service. The Supplier will use diligent efforts to remedy such breach of security or unauthorized access in a timely manner. In the event of any breach of this Attachment, the Supplier shall notify the Bank promptly ( ) upon becoming aware thereof.
13. *Remedies.* The Supplier understands that failure to carry out the requirements of this Agreement may result in the exercise of all remedies at law or equity available to the Bank.



**ATTACHMENT 1-D**

## Reserve Bank Personally Identifiable Information Covenants for Access to Low or Very Low PII Elements

**DEFINITIONS**

“**Incident**” means any actual or suspected loss, unauthorized disclosure, use, acquisition of, or access to Reserve Bank PII by Subcontractor or any of its Staff or Third parties whether in paper or electronic format.

“**Low PII Elements**” means any of the following elements:

- Salary or compensation information
- Personal cell phone number
- Personal email
- Other financial information (loan number, amount, origination date, etc.)
- Online behavioral (e.g. cookies, web beacons)
- Sexual orientation
- Religion
- Full Physical address
- Race or ethnicity
- Personal IP Address
- License Plate #
- Work and educational history
- Personal landline number
- Age (or age range)
- Marital/family status
- Gender
- Personal device Information

“**Subcontractor**” means a Third party that provides products and/or services to FTI Consulting.

“**Third party**” means an entity or person, other than Subcontractor Staff, that is outside of Subcontractor’s organization, and includes Subcontractor’s Subcontractors.

“**Subcontractor Staff**” means all Subcontractor employees and contingent workers, including non-employees working under the supervision of the Subcontractor, such as temporary staff or individuals assigned by staffing agencies.

“**Very Low PII Elements**” means any of the following elements:

- Demographic Information
- Partial address or other location data
- Name
- Other (Including online and device data)
- City
- State
- Zip Code
- Other location data
- Online identities

**Personally Identifiable Information.**

1. **Definition.** “**Reserve Bank PII**” or “**Reserve Bank Personally Identifiable Information**” means any personal information, in electronic or paper form, maintained or otherwise handled or possessed by Subcontractor on behalf of the Bank and that is linked or linkable to an individual by name or other identifying information. Examples of Reserve Bank PII include, but are not limited to, the following linked or linkable information:
  - Social Security number (including only the last 4 digits), driver’s license, passport, or other government issued identification number;
  - Financial institution account number, with or without access code;
  - Credit or debit card number;
  - Personal contact information, such as address, phone number, personal email account, etc.
  - Health or medical information in electronic or physical form relating to an individual’s medical history, medical treatment, mental or physical condition, or diagnosis, or payment for provision of health care;
  - Biometric data;
  - Date of birth;
  - Parents’ last name at birth;
  - Gender or ethnicity;
  - Personnel records;
  - Password, access code, or other information allowing access to account or network containing other Reserve Bank PII;
  - Investigative records, including financial, law enforcement, and background check; and
  - Compensation or tax information.
2. **Purpose, Use, Access & Sharing.** Subcontractor is prohibited from using Reserve Bank PII for any purpose other than for which it was specifically provided pursuant to this Agreement. Subcontractor shall only share Reserve Bank PII with Subcontractor Staff to the extent such Subcontractor Staff has a need to access the Reserve Bank PII in order to provide the specific Service to the Bank pursuant to this Agreement.
3. **Sharing with Third parties.** In addition, Subcontractor shall not share Reserve Bank PII with Third Parties unless and to the extent Subcontractor:
  - (a) has performed and documented due diligence on such Third Parties to ensure appropriate protection, handling, use, sharing retention and deletion of PII disclosed to such Third Parties that are consistent with or comparable to the requirements that apply to Subcontractor pursuant to this Attachment;
  - (b) ensures that all Third Parties do not transmit Reserve Bank PII to any entity outside of the United States or store Reserve Bank PII outside of the United States;
  - (c) has signed agreements with each such Subcontractors that contain provisions substantially similar to those in this Attachment for Reserve Bank PII;
  - (d) engages in ongoing monitoring of such Subcontractors to ensure effective Subcontractor implementation and continuing application of all applicable requirements; and

- (e) within 14 days after the Bank's request provides to the Bank a list of Subcontractors with access to Reserve Bank PII and an attestation that the Subcontractor has complied with the requirements of this Attachment with respect to these Subcontractors.
4. Geographic Limitations. Subcontractor is prohibited from transmitting Reserve Bank PII to any Third party located outside of the United States and from accessing, storing, and processing Reserve Bank PII on servers and other devices located outside of the United States.
5. Minimization. Subcontractor agrees to minimize the collection, acquisition, processing, sharing, and retention of Reserve Bank PII to what is necessary for purposes of providing the specific Service to the Bank pursuant to this Agreement.
6. Destruction and/or Return of Reserve Bank PII. The Subcontractor agrees to destroy all Reserve Bank PII as soon as it is no longer necessary to satisfy the purpose for which the Reserve Bank PII was obtained pursuant to this Agreement, or two business days after termination or expiration of this Agreement, whichever is later. This requirement does not apply to the extent: (a) otherwise specifically provided in this Agreement; (b) required to be retained longer by the Subcontractor pursuant to applicable court order or state or federal laws or regulations, in which case Subcontractor will notify the Bank of what is retained, where and for how long; or (c) otherwise instructed in writing by the Bank, which may include the secure delivery of Reserve Bank PII to the Bank in lieu of destruction.
- (i) The Subcontractor's obligation to destroy pursuant to this Section [TBD] includes all copies, back-ups, and iterations of Reserve Bank PII regardless of (A) the format in which it is retained; (B) the type of device on which, or location where, it is stored; and (C) whether it is retained or held by the Subcontractor, Subcontractor Staff, or a Subcontractor.
- (ii) Destruction pursuant to this provision means the definitive obliteration of Reserve Bank PII in all media that ensures that it cannot be retrieved, recreated, reassembled, or reconstructed.
7. Notification of Incidents involving PII. The Subcontractor must notify the Bank promptly ( ) when the Subcontractor, Subcontractor Staff, or Third parties become aware of an Incident. This notification must occur without delay on account of business hours, holiday or otherwise, even if it means notifying the Bank before the Subcontractor has commenced or completed its own investigation into the cause or extent of the Incident. Notice should be given to the Bank pursuant to the notice provision of this Agreement. Subcontractor shall report any Incident regardless of whether the Incident appears to present a risk of harm or loss. Subcontractor agrees to promptly (a) investigate the Incident; (b) act on the Bank's request for investigative steps; (c) regularly report detailed findings as to the cause and impact of the Incident; (d) cooperate with the Bank in its efforts to remediate and make proper notifications to individuals; and (e) upon the Bank's request, promptly provide progress reports regarding any investigation and/or remediation efforts.
8. Specific Information Security Requirements. In addition to the General Information Security Program standards above, Subcontractor, Subcontractor Staff, and Subcontractors

shall comply with the following authorizations and minimum standards when accessing, using or storing Reserve Bank PII:

- (a) *Minimum Standards for Storage on Laptops and Mobile Computing and Mobile Storage Devices.* Subcontractor must have written policies requiring the use of encryption and physical access controls (e.g., within a locked office, desk, filing cabinet, or file room) for storage on laptops and mobile computing and mobile storage devices.
- (b) *Minimum Standards for Printing.* Printed Reserve Bank PII requires a conspicuous label that Subcontractor would ordinarily use to indicate the sensitivity and confidentiality of its own information. Where technically and operationally feasible, the labeling or marking must be on every page, including any cover memorandums or title pages. Otherwise, a conspicuous cover sheet labeled or marked as Subcontractor would its own sensitive and confidential information must be attached.
- (c) *Minimum Standards for Marking Digital Versions.* A label indicating that the data or digital information is sensitive and confidential must be provided when the Reserve Bank PII is to be accessed or displayed on screen. Where technically and operationally feasible, a label commensurate with what Subcontractor would use to indicate the sensitivity and confidentiality of its own information should be included within the header of a document or at the top of a screen or page of web content; otherwise, a banner label must be displayed on the login screen of systems containing Reserve Bank PII, or on the first screen after login. The banner label must conspicuously state that the system contains sensitive and confidential information and that by continuing, the user acknowledges that unlabeled information within the system must be handled appropriately.
- (d) *Minimum Standards for Transmission.* Reserve Bank PII in digital form, including email and fax, must be encrypted during transmission.
- (e) *Minimum Standards for Storage in Print and Digital Formats.* Storage of Reserve Bank PII information on printed media requires physical access controls (e.g., within a locked office, desk, filing cabinet, or file room). Storage of Reserve Bank PII information on fixed media requires the use of technical access controls. Reserve Bank PII in digital form must be encrypted, tokenized or masked at rest throughout its lifecycle according to the highest industry standards.
- (f) *Minimum Standards for Media Sanitation.* Reserve Bank PII stored on electronic media or similar equipment to be reused, repaired, or disposed of must be cleansed or sanitized using a secure method (e.g., degaussing or data overwrite). This includes computers, and any other devices that have memory or storage that may contain Reserve Bank PII.
- (g)

10. Privacy.

- (a) The Subcontractor must maintain effective privacy policies, processes, and procedures during the term of this Agreement to ensure compliance with the provisions in this Section [TBD]. Subcontractor must actively monitor for compliance with agreed upon requirements for Reserve Bank PII, including tracking and mitigating instances of non-compliance.
- (b) The Subcontractor agrees to maintain an appropriate privacy notice that is easily accessible and prominently displayed at the point(s) it collects Reserve Bank PII from individuals. The privacy notice must, at a minimum, describe the types of PII collected, the purpose(s) for which PII is collected, the intended use(s) of PII, and generally, how PII is shared internally and externally. If the Subcontractor changes its privacy notice, the Subcontractor shall promptly notify the Bank thereof and provide the Bank with the updated notice.
- (c) Where applicable, the privacy notices will also provide information relating to the type and method for consent offered to individuals. Any use of Reserve Bank PII for purposes other than providing the services to the Reserve Bank pursuant to this Agreement must be agreed to by the individuals providing the PII through opt-in or express consent, where the individuals must take affirmative action beyond just submitting the information, to agree to such other use or disclosure of the PII.

14. DSR Responses. Subcontractor shall also promptly respond to and implement any data subject request (DSRs) with respect to any Reserve Bank PII (but in any event, not longer than 5 business days after request by the Bank, unless such time period is extended in the sole direction of the Bank).

Subcontractor's activities pursuant to this Attachment shall be undertaken at no cost to the Reserve Bank.

**ATTACHMENT 1-E**

## Reserve Bank Personally Identifiable Information Covenants for Access to Moderate PII Elements

**DEFINITIONS**

“**Incident**” means any actual or suspected loss, unauthorized disclosure, use, acquisition of, or access to Reserve Bank PII by Subcontractor or any of its Staff or Third parties whether in paper or electronic format.

“**Moderate PII Elements**” mean any of the following elements:

- Biometric information
- Account number (deposit account at financial institution)
- Date of Birth
- Investigative records, including financial, law enforcement, and background check
- Credit rating information
- Parent’s last name at birth (aka maiden name)
- Performance review/disciplinary action
- Credit card number
- Precise geolocation (e.g. latitude longitude)
- Benefit information (benefits selection, claims information, etc.)

“**Subcontractor**” means a Third party that provides products and/or services to FTI Consulting.

“**Third party**” means an entity or person, other than Subcontractor Staff, that is outside of Subcontractor’s organization, and includes Subcontractor’s Subcontractors.

“**Subcontractor Staff**” means all Subcontractor employees and contingent workers, including non-employees working under the supervision of the Subcontractor, such as temporary staff or individuals assigned by staffing agencies.

**Personally Identifiable Information.**

1. **Definition.** “**Reserve Bank PII**” or “**Reserve Bank Personally Identifiable Information**” means any personal information, in electronic or paper form, maintained or otherwise handled or possessed by Subcontractor on behalf of the Bank and that is linked or linkable to an individual by name or other identifying information. Examples of Reserve Bank PII include, but are not limited to, the following linked or linkable information:

- Social Security number (including only the last 4 digits), driver’s license, passport, or other government issued identification number;
- Financial institution account number, with or without access code;
- Credit or debit card number;
- Personal contact information, such as address, phone number, personal email account, etc.
- Health or medical information in electronic or physical form relating to an individual’s medical history, medical treatment, mental or physical condition, or diagnosis, or payment for provision of health care;
- Biometric data;
- Date of birth;
- Parents’ last name at birth;
- Gender or ethnicity;
- Personnel records;

- Password, access code, or other information allowing access to account or network containing other Reserve Bank PII;
  - Investigative records, including financial, law enforcement, and background check; and
  - Compensation or tax information.
9. Purpose, Use, Access & Sharing. Subcontractor is prohibited from using Reserve Bank PII for any purpose other than for which it was specifically provided pursuant to this Agreement. Subcontractor shall only share Reserve Bank PII with Subcontractor Staff to the extent such Subcontractor Staff has a need to access the Reserve Bank PII in order to provide the specific Service to the Bank pursuant to this Agreement. Subcontractor must require Subcontractor Staff with access to Reserve Bank PII to comply with Subcontractor's information security and data privacy requirements, including those that satisfy the requirements of this Attachment.
10. Sharing with Third parties. In addition, Subcontractor shall not share Reserve Bank PII with Third Parties unless and to the extent Subcontractor:
- (f) has performed and documented due diligence on such Third Parties to ensure appropriate protection, handling, use, sharing retention and deletion of PII disclosed to such Third Parties that are consistent with or comparable to the requirements that apply to Subcontractor pursuant to this Attachment;
  - (g) ensures that all Third Parties do not transmit Reserve Bank PII to any entity outside of the United States or store Reserve Bank PII outside of the United States;
  - (h) has signed agreements with each such Subcontractors that contain provisions substantially similar to those in this Attachment for Reserve Bank PII;
  - (i) engages in ongoing monitoring of such Subcontractors to ensure effective Subcontractor implementation and continuing application of all applicable requirements; and
  - (j) within 14 days after the Bank's request provides to the Bank a list of Subcontractors with access to Reserve Bank PII and an attestation that the Subcontractor has complied with the requirements of this Attachment with respect to these Subcontractors.
11. Geographic Limitations. Subcontractor is prohibited from transmitting Reserve Bank PII to any Third party located outside of the United States and from accessing, storing, and processing Reserve Bank PII on servers and other devices located outside of the United States.
12. Minimization. Subcontractor agrees to minimize the collection, acquisition, processing, sharing, and retention of Reserve Bank PII to what is necessary for purposes of providing the specific Service to the Bank pursuant to this Agreement.
13. Destruction and/or Return of Reserve Bank PII. The Subcontractor agrees to destroy all Reserve Bank PII as soon as it is no longer necessary to satisfy the purpose for which the Reserve Bank PII was obtained pursuant to this Agreement, or two business days after termination or expiration of this Agreement, whichever is later. This requirement does not apply to the extent: (a) otherwise specifically provided in this Agreement; (b) required to be retained longer by the Subcontractor pursuant to applicable court order or state or federal

laws or regulations, in which case Subcontractor will notify the Bank of what is retained, where and for how long; or (c) otherwise instructed in writing by the Bank, which may include the secure delivery of Reserve Bank PII to the Bank in lieu of destruction.

- (iii) The Subcontractor's obligation to destroy pursuant to this Section [TBD] includes all copies, back-ups, and iterations of Reserve Bank PII regardless of (A) the format in which it is retained; (B) the type of device on which, or location where, it is stored; and (C) whether it is retained or held by the Subcontractor, Subcontractor Staff, or a Subcontractor.
  - (iv) Destruction pursuant to this provision means the definitive obliteration of Reserve Bank PII in all media that ensures that it cannot be retrieved, recreated, reassembled, or reconstructed.
14. Notification of Incidents involving PII. The Subcontractor must notify the Bank promptly ( ) when the Subcontractor, Subcontractor Staff, or Third parties become aware of an Incident. This notification must occur without delay on account of business hours, holiday or otherwise, even if it means notifying the Bank before the Subcontractor has commenced or completed its own investigation into the cause or extent of the Incident. Notice should be given to the Bank pursuant to the notice provision of this Agreement. Subcontractor shall report any Incident regardless of whether the Incident appears to present a risk of harm or loss. Subcontractor agrees to promptly (a) investigate the Incident; (b) act on the Bank's request for investigative steps; (c) regularly report detailed findings as to the cause and impact of the Incident; (d) cooperate with the Bank in its efforts to remediate and make proper notifications to individuals; and (e) upon the Bank's request, promptly provide progress reports regarding any investigation and/or remediation efforts.
15. Specific Information Security Requirements. In addition to the General Information Security Program standards above, Subcontractor, Subcontractor Staff, and Subcontractors shall comply with the following authorizations and minimum standards when accessing, using or storing Reserve Bank PII:
- (a) *Minimum Standards for Storage on Laptops and Mobile Computing and Mobile Storage Devices.* Subcontractor must have written policies requiring the use of encryption and physical access controls (e.g., within a locked office, desk, filing cabinet, or file room) for storage on laptops and mobile computing and mobile storage devices.
  - (c) *Minimum Standards for Printing.* Printed Reserve Bank PII requires a conspicuous label that Subcontractor would ordinarily use to indicate the sensitivity and confidentiality of its own information. Where technically and operationally feasible, the labeling or marking must be on every page, including any cover memorandums or title pages. Otherwise, a conspicuous cover sheet labeled or marked as Subcontractor would its own sensitive and confidential information must be attached.
  - (h) *Minimum Standards for Marking Digital Versions.* A label indicating that the data or digital information is sensitive and confidential must be provided when the Reserve Bank PII is to be accessed or displayed on screen. Where technically and operationally feasible, a label commensurate with what Subcontractor would use to indicate the



sensitivity and confidentiality of its own information should be included within the header of a document or at the top of a screen or page of web content; otherwise, a banner label must be displayed on the login screen of systems containing Reserve Bank PII, or on the first screen after login. The banner label must conspicuously state that the system contains sensitive and confidential information and that by continuing, the user acknowledges that unlabeled information within the system must be handled appropriately.

- (i) *Minimum Standards for Transmission.* Reserve Bank PII in digital form, including email and fax, must be encrypted during transmission.
- (j) *Minimum Standards for Storage in Print and Digital Formats.* Storage of Reserve Bank PII information on printed media requires physical access controls (e.g., within a locked office, desk, filing cabinet, or file room). Storage of Reserve Bank PII information on fixed media requires the use of technical access controls. Reserve Bank PII in digital form must be encrypted, tokenized or masked at rest throughout its lifecycle according to the highest industry standards.
- (k) *Minimum Standards for Media Sanitation.* Reserve Bank PII stored on electronic media or similar equipment to be reused, repaired, or disposed of must be cleansed or sanitized using a secure method (e.g., degaussing or data overwrite). This includes computers, and any other devices that have memory or storage that may contain Reserve Bank PII.
- (l)

10. Privacy.

- (d) The Subcontractor must maintain effective privacy policies, processes, and procedures during the term of this Agreement to ensure compliance with the provisions in this Section [TBD]. Subcontractor must actively monitor for compliance with agreed upon requirements for Reserve Bank PII, including tracking and mitigating instances of non-compliance.
- (e) The Subcontractor agrees to maintain an appropriate privacy notice that is easily accessible and prominently displayed at the point(s) it collects Reserve Bank PII from individuals. The privacy notice must, at a minimum, describe the types of PII collected, the purpose(s) for which PII is collected, the intended use(s) of PII, and generally, how PII is shared internally and externally. If the Subcontractor changes its privacy notice, the Subcontractor shall promptly notify the Bank thereof and provide the Bank with the updated notice.
- (f) Where applicable, the privacy notices will also provide information relating to the type and method for consent offered to individuals. Any use of Reserve Bank PII for purposes other than providing the services to the Reserve Bank pursuant to this Agreement must be agreed to by the individuals providing the PII through opt-in or

express consent, where the individuals must take affirmative action beyond just submitting the information, to agree to such other use or disclosure of the PII.

- (g) The parties acknowledge and agree that Subcontractor shall comply with all laws, rules and regulations applicable to the Subcontractor's performance of Services pursuant to this Agreement. Subcontractor acknowledges and confirms that it does not provide Company or Bank with any monetary or other valuable consideration in exchange for Reserve Bank PII and certifies that it understands and will comply with the restrictions set forth herein. Except as required by applicable law, regulation, or professional standard, Subcontractor will not collect, access, use, disclose, process, or retain Reserve Bank PII for any purpose other than the purpose of performing the Services and this Agreement. In particular, Subcontractor shall not sell (as defined by applicable data protection laws) any Reserve Bank PII. Subcontractor will, to the extent legally permissible, notify Bank and Company if Subcontractor receives a request from a data subject of Reserve Bank PII seeking to exercise such data subject's rights under any applicable data protection laws ("Data Subject Access Request"), and will, on Bank's or Company's reasonable request, provide reasonable assistance in connection with their response to such Data Subject Access Request
11. Indemnification. Notwithstanding any limitation on indemnification or damages provided elsewhere in this Agreement, the Subcontractor shall be liable for and agrees to indemnify, defend, and hold the Bank harmless from any costs or fees of data recovery, Incident investigation, third party liability, government imposed actions or penalties, and notification and identity theft protection services offered to affected individuals, arising from, or related to, any Incident involving Reserve Bank PII, the determination of which will be made in the sole discretion of the Bank. If requested by the Bank, the Subcontractor-paid identity theft protection services shall be provided through the Bank's designated identity theft protection service provider.
14. DSR Responses. Subcontractor shall also promptly respond to and implement any data subject request (DSRs) with respect to any Reserve Bank PII (but in any event, not longer than 5 business days after request by the Bank, unless such time period is extended in the sole direction of the Bank).

Subcontractor's activities pursuant to this Attachment shall be undertaken at no cost to the Reserve Bank.

**ATTACHMENT 1-F**

## Reserve Bank Personally Identifiable Information Covenants for Access to High PII Elements

**DEFINITIONS**

“**High PII Elements**” mean any of the following elements:

- SSN (including just last four digits)
- Health and medical information
- Password or access code
- Driver’s license number or other government ID number
- Passport number

“**Incident**” means any actual or suspected loss, unauthorized disclosure, use, acquisition of, or access to Reserve Bank PII by Subcontractor or any of its Staff or Third parties whether in paper or electronic format.

“**Subcontractor**” means a Third party that provides products and/or services to FTI Consulting.

“**Third party**” means an entity or person, other than Subcontractor Staff, that is outside of Subcontractor’s organization, and includes Subcontractor’s Subcontractors.

“**Subcontractor Staff**” means all Subcontractor employees and contingent workers, including non-employees working under the supervision of the Subcontractor, such as temporary staff or individuals assigned by staffing agencies.

**Personally Identifiable Information.**

1. Definition. “**Reserve Bank PII**” or “**Reserve Bank Personally Identifiable Information**” means any personal information, in electronic or paper form, maintained or otherwise handled or possessed by Subcontractor on behalf of the Bank and that is linked or linkable to an individual by name or other identifying information. Examples of Reserve Bank PII include, but are not limited to, the following linked or linkable information:

- Social Security number (including only the last 4 digits), driver’s license, passport, or other government issued identification number;
- Financial institution account number, with or without access code;
- Credit or debit card number;
- Personal contact information, such as address, phone number, personal email account, etc.
- Health or medical information in electronic or physical form relating to an individual’s medical history, medical treatment, mental or physical condition, or diagnosis, or payment for provision of health care;
- Biometric data;
- Date of birth;
- Parents’ last name at birth;
- Gender or ethnicity;
- Personnel records;
- Password, access code, or other information allowing access to account or network containing other Reserve Bank PII;
- Investigative records, including financial, law enforcement, and background check; and
- Compensation or tax information.

16. Purpose, Use, Access & Sharing. Subcontractor is prohibited from using Reserve Bank PII for any purpose other than for which it was specifically provided pursuant to this Agreement. Subcontractor shall only share Reserve Bank PII with Subcontractor Staff to the extent such Subcontractor Staff has a need to access the Reserve Bank PII in order to provide the specific Service to the Bank pursuant to this Agreement. Subcontractor must require Subcontractor Staff with access to Reserve Bank PII to comply with Subcontractor's information security and data privacy requirements, including those that satisfy the requirements of this Attachment.
17. Sharing with Third parties. In addition, Subcontractor shall not share Reserve Bank PII with Third Parties unless and to the extent Subcontractor:
  - (k) has performed and documented due diligence on such Third Parties to ensure appropriate protection, handling, use, sharing retention and deletion of PII disclosed to such Third Parties that are consistent with or comparable to the requirements that apply to Subcontractor pursuant to this Attachment;
  - (l) ensures that all Third Parties do not transmit Reserve Bank PII to any entity outside of the United States or store Reserve Bank PII outside of the United States;
  - (m) has signed agreements with each such Subcontractors that contain provisions substantially similar to those in this Attachment for Reserve Bank PII;
  - (n) engages in ongoing monitoring of such Subcontractors to ensure effective Subcontractor implementation and continuing application of all applicable requirements; and
  - (o) within 14 days after the Bank's request provides to the Bank a list of Subcontractors with access to Reserve Bank PII and an attestation that the Subcontractor has complied with the requirements of this Attachment with respect to these Subcontractors.
18. Geographic Limitations. Subcontractor is prohibited from transmitting Reserve Bank PII to any Third party located outside of the United States and from accessing, storing, and processing Reserve Bank PII on servers and other devices located outside of the United States.
19. Minimization. Subcontractor agrees to minimize the collection, acquisition, processing, sharing, and retention of Reserve Bank PII to what is necessary for purposes of providing the specific Service to the Bank pursuant to this Agreement.
20. Destruction and/or Return of Reserve Bank PII. The Subcontractor agrees to destroy all Reserve Bank PII as soon as it is no longer necessary to satisfy the purpose for which the Reserve Bank PII was obtained pursuant to this Agreement, or two business days after termination or expiration of this Agreement, whichever is later. This requirement does not apply to the extent: (a) otherwise specifically provided in this Agreement; (b) required to be retained longer by the Subcontractor pursuant to applicable court order or state or federal laws or regulations, in which case Subcontractor will notify the Bank of what is retained, where and for how long; or (c) otherwise instructed in writing by the Bank, which may include the secure delivery of Reserve Bank PII to the Bank in lieu of destruction.

- (v) The Subcontractor's obligation to destroy pursuant to this Section [TBD] includes all copies, back-ups, and iterations of Reserve Bank PII regardless of (A) the format in which it is retained; (B) the type of device on which, or location where, it is stored; and (C) whether it is retained or held by the Subcontractor, Subcontractor Staff, or a Subcontractor.
  - (vi) Destruction pursuant to this provision means the definitive obliteration of Reserve Bank PII in all media that ensures that it cannot be retrieved, recreated, reassembled, or reconstructed.
21. Notification of Incidents involving PII. The Subcontractor must notify the Bank promptly ( ) when the Subcontractor, Subcontractor Staff, or Third parties become aware of an Incident. This notification must occur without delay on account of business hours, holiday or otherwise, even if it means notifying the Bank before the Subcontractor has commenced or completed its own investigation into the cause or extent of the Incident. Notice should be given to the Bank pursuant to the notice provision of this Agreement. Subcontractor shall report any Incident regardless of whether the Incident appears to present a risk of harm or loss. Subcontractor agrees to promptly (a) investigate the Incident; (b) act on the Bank's request for investigative steps; (c) regularly report detailed findings as to the cause and impact of the Incident; (d) cooperate with the Bank in its efforts to remediate and make proper notifications to individuals; and (e) upon the Bank's request, promptly provide progress reports regarding any investigation and/or remediation efforts.
- 22.
23. Specific Information Security Requirements. In addition to the General Information Security Program standards above, Subcontractor, Subcontractor Staff, and Subcontractors shall comply with the following authorizations and minimum standards when accessing, using or storing Reserve Bank PII:
- (a) *Minimum Standards for Storage on Laptops and Mobile Computing and Mobile Storage Devices.* Subcontractor must have written policies requiring the use of encryption and physical access controls (e.g., within a locked office, desk, filing cabinet, or file room) for storage on laptops and mobile computing and mobile storage devices.
  - (d) *Minimum Standards for Printing.* Printed Reserve Bank PII requires a conspicuous label that Subcontractor would ordinarily use to indicate the sensitivity and confidentiality of its own information. Where technically and operationally feasible, the labeling or marking must be on every page, including any cover memorandums or

title pages. Otherwise, a conspicuous cover sheet labeled or marked as Subcontractor would its own sensitive and confidential information must be attached.

- (m) *Minimum Standards for Marking Digital Versions.* A label indicating that the data or digital information is sensitive and confidential must be provided when the Reserve Bank PII is to be accessed or displayed on screen. Where technically and operationally feasible, a label commensurate with what Subcontractor would use to indicate the sensitivity and confidentiality of its own information should be included within the header of a document or at the top of a screen or page of web content; otherwise, a banner label must be displayed on the login screen of systems containing Reserve Bank PII, or on the first screen after login. The banner label must conspicuously state that the system contains sensitive and confidential information and that by continuing, the user acknowledges that unlabeled information within the system must be handled appropriately.
- (n) *Minimum Standards for Transmission.* Reserve Bank PII in digital form, including email and fax, must be encrypted during transmission.
- (o) *Minimum Standards for Storage in Print and Digital Formats.* Storage of Reserve Bank PII information on printed media requires physical access controls (e.g., within a locked office, desk, filing cabinet, or file room). Storage of Reserve Bank PII information on fixed media requires the use of technical access controls. Reserve Bank PII in digital form must be encrypted, tokenized or masked at rest throughout its lifecycle according to the highest industry standards.
- (p) *Minimum Standards for Media Sanitation.* Reserve Bank PII stored on electronic media or similar equipment to be reused, repaired, or disposed of must be cleansed or sanitized using a secure method (e.g., degaussing or data overwrite). This includes computers, and any other devices that have memory or storage that may contain Reserve Bank PII.
- (q)

## 10. Privacy.

- (h) The Subcontractor must maintain effective privacy policies, processes, and procedures during the term of this Agreement to ensure compliance with the provisions in this Section [TBD]. Subcontractor must actively monitor for compliance with agreed upon requirements for Reserve Bank PII, including tracking and mitigating instances of non-compliance.
- (i) The Subcontractor agrees to maintain an appropriate privacy notice that is easily accessible and prominently displayed at the point(s) it collects Reserve Bank PII from individuals. The privacy notice must, at a minimum, describe the types of PII collected, the purpose(s) for which PII is collected, the untended use(s) of PII, and generally, how PII is shared internally and externally. If the Subcontractor changes

its privacy notice, the Subcontractor shall promptly notify the Bank thereof and provide the Bank with the updated notice.

- (j) Where applicable, the privacy notices will also provide information relating to the type and method for consent offered to individuals. Any use of Reserve Bank PII for purposes other than providing the services to the Reserve Bank pursuant to this Agreement must be agreed to by the individuals providing the PII through opt-in or express consent, where the individuals must take affirmative action beyond just submitting the information, to agree to such other use or disclosure of the PII.
  - (k) Where options for consents are provided in the privacy notice, the Subcontractor must implement processes to ensure that each individual's consent and preferences are documented and tracked, and that the preferences are implemented and honored.
  - (l) The parties acknowledge and agree that Subcontractor is acting as a service provider (as such term is defined by the California Consumer Privacy Act of 2018 ("CCPA")) to Bank and Company in connection with Subcontractor's performance of Services pursuant to this Agreement. Subcontractor acknowledges and confirms that it does not provide Company or Bank with any monetary or other valuable consideration in exchange for Reserve Bank PII and certifies that it understands and will comply with the restrictions set forth herein. Except as required by applicable law, regulation, or professional standard, Subcontractor will not collect, access, use, disclose, process, or retain Reserve Bank PII for any purpose other than the purpose of performing the Services or another business purpose permitted by 11 CCR § 999.314(c) and this Agreement. In particular, Subcontractor shall not sell (as defined by applicable data protection laws, including without limitation and to the extent applicable, the CCPA) any Reserve Bank PII. Subcontractor will, to the extent legally permissible, notify Bank and Company if Subcontractor receives a request from a data subject of Reserve Bank PII seeking to exercise such data subject's rights under any applicable data protection laws ("Data Subject Access Request"), and will, on Bank's or Company's reasonable request, provide reasonable assistance in connection with their response to such Data Subject Access Request
12. Audit Logs. The Subcontractor will maintain audit logs of all access to Reserve Bank PII and will actively monitor them for unauthorized access.
13. Indemnification. Notwithstanding any limitation on indemnification or damages provided elsewhere in this Agreement, the Subcontractor shall be liable for and agrees to indemnify, defend, and hold the Bank harmless from all costs and/or damages arising from, or related to, any Incident involving Reserve Bank PII including, but not limited to, any costs of data recovery, Incident investigation, third party liability, government imposed actions or penalties, and notification and identity theft protection services offered to affected individuals, the determination of which will be made in the sole discretion of the Bank. If requested by the Bank, the Subcontractor-paid identity theft protection services shall be provided through the Bank's designated identity theft protection service provider.
14. Audit. The Bank shall have the right to audit Subcontractor's overall privacy and information security program and its compliance with the requirements in this Attachment at the commencement of Services and on annual basis during the term of this Agreement; provided that following an Incident, the Bank shall have the right to conduct such audit

upon reasonable request. During the performance of the Services, on an ongoing basis from time to time and with no less than ten days' notice, the Bank, at its own expense, shall be entitled to perform, or to have performed, an on-site audit of Subcontractor's privacy [and/or] information security program. In lieu of or in addition to an on-site audit, the Reserve Bank in its sole discretion may require the Subcontractor to complete an audit questionnaire provided by the Reserve Bank regarding Subcontractor's compliance. Subcontractor shall complete such audit questionnaire within 45 calendar days of receipt of the Reserve Bank's request. The Reserve Bank may conduct such audits using employees, agents, representatives, contractors, or designees of the Reserve Bank or of the Board of Governors of the Federal Reserve System.

Subcontractor agrees to work in good faith with the Reserve Bank to promptly address/remedy any areas of concern or of non-compliance identified by the Reserve Bank as a result of an audit in order for the Reserve Bank to satisfy its ongoing oversight of its relationship with Subcontractor. In the event that parties are unable to mutually agree on appropriate remedies, or Subcontractor does not adequately remediate, or agree to remediate, areas of concern or non-compliance within 45 days of receipt of the audit, the Reserve Bank may terminate this Agreement for cause.

14. DSR Reponses. Subcontractor shall also promptly respond to and implement any data subject request (DSRs) with respect to any Reserve Bank PII (but in any event, not longer than 5 business days after request by the Bank, unless such time period is extended in the sole direction of the Bank).

Subcontractor's activities pursuant to this Attachment shall be undertaken at no cost to the Reserve Bank.