

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

for

Financial Advisory Services - Marketing & Sales Loan Assets III

Sandler, O'Neill & Partners, LP

(RECVR-15-G-0320)



Date Approved by Chief Privacy Officer (CPO)/Designee: 6/6/2016

PTA/PIA TEMPLATE VERSION 1.6 - March 2016

SECTION I – OUTSOURCED INFORMATION SERVICE DESCRIPTION

1. Describe the outsourced service and its purpose.

The FDIC maintains stability and public confidence in the nation's financial system by insuring deposits, examining and supervising financial institutions (FIs), and managing receiverships. The FDIC Division of Resolutions and Receiverships (DRR) is responsible for resolving failed or failing FDIC-insured depository FIs, which include among other important responsibilities, effectively and efficiently managing and disposing assets held by the FIs.

FDIC DRR has contracted the financial advisory services of Sandler O'Neill & Partners, LP (Sandler) to support the overall disposition of assigned assets from failing or failed FDIC-insured depository FIs which include financial analysis, valuation, and marketing and sales. Depending on the situation surrounding one or more failed or failing FIs, the FDIC may require the contractor to be involved in pre-failure financial advisory tasks, post-failure advisory task, or both pre-failure and post-failure advisory tasks.

In a pre-failure scenario, the assigned assets are derived from one or more failing FIs which may ultimately not fail. The associated task areas for pre-failure services may include reviewing and analyzing initial loan level files and any related imaged loan documents, preparing a summary report advising the FDIC with recommendations on liquidation strategies to include options such as structured sales with or without leverage and/or cash options, and continue ongoing surveillance of the assigned assets.

Upon completion of pre-failure services, the FI may ultimately fail and its assets assigned to FDIC receivership. If the FDIC decides to implement one or more of the recommended strategies set forth by Sandler, the contractor would transition to post-failure services. Post-failure activities may include reviewing information regarding the inventory of the assigned assets and preliminary aggregation of the portfolio; recommending the scope/sample size of the loan data reviews and due diligence information; obtaining asset due diligence information from documentation provided by FDIC needed to market the assigned assets to potential bidders; recommending a best execution strategy to the FDIC based on the loan data review and due diligence results; advising FDIC on the continued uses of its partnership structure and making recommendations for other potential structures; and executing marketing and sales campaigns.

2. Status of the Outsourced Information Service Provider:

- Solicitation/On-Boarding (Pre-Award; or At/Around the Time of Contract Award)
- Initial Assessment/Due Diligence (Post-Award)
- Ongoing Monitoring of Contract (Post-Award)
- Sunset or Disposition of Contract (Post-Award; At or Near Contract Expiration)
- Other (*Explain*):

SECTION II – DATA TYPE, SOURCES, AND USE

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

Sandler personnel review and utilize the assigned asset data provided by the FDIC via the FDIC VDR¹, which may include PII about borrowers/customers of a failing or failed FI. FDIC Business Information Systems (BIS) staff uploads failing/failed bank data to an internal FDIC SharePoint site. From there, the FDIC DRR Franchise and Asset Marketing Branch (FAMB)² Capital Markets Group retrieve the data from the SharePoint site and provide Sandler with the assigned asset data in the form of electronic imaged loan files with read-only access on the FDIC VDR. This personally identifiable information (PII) may include the borrower's/customer's full name, date of birth, social security number (SSN), employment status, home address, personal phone number, personal email address, financial information, vehicle identifiers, legal documents, and military status/records. This data is utilized by authorized Sandler personnel to provide the FDIC with loan summary reports, loan summary relationship reports, and asset valuation and disposition reports. The final advisory valuation assessments (reports) prepared by Sandler contain a limited amount of the aforementioned PII.

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

Sandler personnel utilize the assigned asset data described above in order to provide the FDIC with financial valuation reports and advice concerning a failing or failed FI's loan assets. Sandler assesses current market conditions regarding loan assets and provides a range of values and disposition strategies for each class of loans in their valuation reports. These assessments are utilized by the FDIC to resolve loan assets in a manner that is most cost-effective for the Deposit Insurance Fund (DIF) Reserve³.

In addition to conducting valuations of loan assets and making recommendations for other potential structures, Sandler may be tasked with executing marketing and sales campaigns for the assigned assets. After the closing of a failed FI, the FDIC may decide to implement one or more of the recommended strategies set forth by Sandler after approval from the FDIC Oversight Manager. Sandler receives asset due diligence information from documentation provided by FDIC in order to market the assigned assets via the FDIC VDR. Sandler facilitates FDIC VDR access for potential bidders to view the loan level data in order to submit bids via FDIC-granted permissions. The

¹ The FDIC's VDR is a secure website facility and technology provided by a private sector service provider (FDIC is currently using RR Donnelly's VDR known as Venue). The VDR service is used by DRR to create workspaces for failing or failed FI projects, where confidential documents and information can be rapidly exchanged with specific groups of authorized internal and external users. For example, DRR staff use the VDR to provide extensive information to bidders about the failing FI and the marketing process. Loan and deposit database files, general ledgers and other performance reports, as well as detailed operations information, are provided on the secured website. DRR staff may also provide imaged loan files for larger failing FIs if time permits. The VDR is also used to share information with regulators on bidder activity to ensure that interested bidders are eligible to bid. For additional information, refer to the FDIC's VDR Privacy Impact Assessment at www.fdic.gov.

² The DRR Franchise and Asset Marketing Branch (FAMB) supports the franchise marketing process by providing data processing services related to the failing institution

³ DIF Reserve – Deposit Insurance Fund Reserve insures the deposits and protects the depositors of insured banks and to resolve failed banks. The Federal Deposit Insurance Act requires the FDIC's Board to set the Designated Reserve Ratio (DRR) for the DIF annually. Since 2010, the Board has adopted a 2.0 percent DRR each year. A bank's assessment is calculated by multiplying its assessment rate by its assessment base. A bank's assessment base and assessment rate are determined each quarter.

investors send bids, which do not contain PII, in the form of Excel spreadsheets via email to Sandler. Sandler, as the financial advisor, decides the most suitable bid and sends the investor data to the FDIC. After approval by the FDIC, the loan sale is executed.

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

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

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

Estimated Number of Records Containing PII				
0	1-500	501-1,000	1,001 - 2,500	2,501 - 5,000
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5,001 - 7,500	7,501 - 10,000	10,000 - 50,000	50,000 - 100,000	over 100,000
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

6b. If “0” was answered for 6a, please explain⁴: The contract technical monitor has confirmed that Sandler has not been issued any active task orders as of 3/14/2016, and does not anticipate any task orders will be awarded until assets are assigned for marketing and sales purposes. An estimate of the number of records that could potentially be maintained if the vendor were assigned work in the future estimating large bank failures is over 100,000.

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

Data Source⁵ (List all sources that the Outsourced Provider collects, obtains or receives data from, as part of the services provided under the contract.)	Type of Data Provided by Source & How It is Derived (Describe the type of PII and non-PII data provided by each source. If PII is included in the data, list the specific PII elements, and explain how the PII is derived.)	Does Data Include PII?
Collected from the FDIC Virtual Data Room (VDR) and the FDIC Secure Email Service	Authorized FDIC/DRR BIS staff uploads failing/failed bank data, which may contain some or all of the PII specified in Q5, to an internal FDIC SharePoint site. From there, the FDIC/DRR FAMB Capital Markets Group retrieves the data from the SharePoint site and provides Sandler with the assigned asset data in the form of electronic imaged loan files with read-only access on the FDIC VDR into Sandler’s respective folder. The information is derived digitally and stored on Sandler’s respective file servers during analysis. In some cases, if Sandler staff requests additional/supplemental valuation information, the FDIC may respond by providing additional information (which may contain PII) via the FDIC VDR, or in certain instances, via the FDIC’s Secure Email Service.	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Collection of Bids from Potential Investors	Sandler facilitates FDIC VDR access for potential bidders to view the loan level data in order to submit bids via FDIC-granted permissions. The investors send bids, which do not contain PII, in the form of Excel spreadsheets via email to Sandler.	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No

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

No

Yes (**Explanation:** The FDIC and the vendor may retrieve data using an individual’s full name or property address.)

Not applicable

⁴ If the vendor has not received work to date for this contract and “0” is checked in 6a, please explain approximately how many records may be maintained by the vendor if they are awarded work under this contract in the future. Additionally, the Division responsible for this vendor must update this PIA to reflect the accurate number of records containing PII that the vendor maintains if this changes in the future.

⁵ Examples of potential data sources include, but are not limited to: internal (FDIC) or external (non-FDIC) systems, websites, individual members of the public (e.g., customers, borrowers, etc.), FDIC employees, FDIC contractors, credit bureaus, commercial entities, public records, government agencies, etc.



This completes the PTA.

- Do not complete the rest of the form, if the service provider is not processing or maintaining sensitive PII. This is the case, if you checked:
 - NOT APPLICABLE for question 3 and NO for all items in question 5; OR
 - Only Full Name in question 5.

- Continue completing the remainder of the form, i.e., Sections III thru VI in their entirety (questions 9 thru 17), if the service provider is processing or maintaining sensitive PII. This is the case, if you checked:
 - YES for Social Security Number (SSN) in question 5; OR
 - YES for SSN or for Full Name in addition to one or more boxes in question 5.

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

SECTION III – DATA ACCESS AND SHARING

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

PII Will Be Accessed By and/or Provided To:	Yes	No	If Yes, Explain How and Why the PII Will Be Accessed/Shared
9a. FDIC Outsourced Service Provider (OSP) Staff; OSP Subcontractors; and/or OSP Systems	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Authorized Sandler staffs that perform work on behalf of the FDIC have access to asset portfolio data, which may contain PII as specified in Question 5, in order to provide valuation assessments and advice regarding FI loan and non-loan assets. Sandler staffs that may have access to PII include: Senior Underwriters and other Underwriters for purposes of making valuation decisions and helping prepare reports; and Financial Analysts for report analysis and preparation.
9b. FDIC Personnel and/or FDIC Systems/ Applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Sandler shares their completed valuation reports and final loan data files (which may contain any of the PII specified in Question 5) with the FDIC via the FDIC VDR. FDIC/DRR FAMB staff has access to the final valuation reports and supporting data files provided by Sandler via the FDIC VDR. Authorized FDIC/DRR personnel post the final reports in a secure FDIC/DRR SharePoint site. These reports are utilized by FDIC/DRR for the purposes detailed in Question 4, such as resolving loan assets in a manner that is most cost-effective, or determining the consideration offered to the potential investor by the FDIC as applicable.
9c. Individual Members of the Public (e.g., bidders, investors, borrowers, customers, etc.)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not Applicable.
9d. Other Non-FDIC Entities/ Parties and/or Non-FDIC Systems/Applications	<input checked="" type="checkbox"/>	<input type="checkbox"/>	After the closing of a failed FI, the FDIC may decide to implement one or more of the recommended strategies set forth by Sandler, which may include executing the marketing and sales campaign of assigned assets after approval by the FDIC Oversight Manager. Sandler receives asset due diligence information from documentation provided by the FDIC in order to market the assigned assets via the FDIC VDR. Sandler facilitates FDIC VDR access for potential bidders to view the loan level data, which may contain PII as specified in Question 5, in order to submit bids via FDIC-granted permissions. The investors send bids, which do not contain PII, in the form of Excel spreadsheets via email to Sandler. Sandler, as the

			financial advisor, decides the most suitable bid and sends the investor data to the FDIC. After approval by the FDIC, the loan sale is executed.
9e. Federal, State, and/or Local Agencies	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not Applicable.
9f. Other	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Not Applicable.

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

Data Protection and/or Sharing Agreements	Yes	No
FDIC Confidentiality Agreement (Corporation)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
FDIC Confidentiality Agreement (Individual)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Non-Disclosure Agreement (NDA)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Memoranda of Understanding (MOU)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Information Sharing Agreements (ISA)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Authentication Risk Assessment	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Other Applicable Agreement(s) (Specify: _____)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<p>If you answered NO to any item above, please provide additional information if available:</p> <p>Sandler is an outsourced service provider and therefore is not subject to MOUs or ISAs.</p>		

SECTION IV – NOTICE AND CONSENT

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

- No. Individuals do not have the opportunity to “opt out” of providing their data and/or consenting to particular uses of their information. **[Explanation: FDIC/DRR has a primary responsibility for resolving failed FDIC insured depository institutions, including the liquidation of assets in receivership. As the sensitive PII from borrowers/customers of failed or failing FIs is derived from bank records in FDIC receivership, individuals do not have an opportunity to opt out or provide consent for the use of the data. The data derived from bank records in FDIC receivership is necessary to help make underwriting decisions, such as whether an applicant is creditworthy and should receive a loan, as well as resolving assets in a manner that is most cost-effective for the DIF Reserve and determining the consideration offered to the potential investor, as applicable.]**

- Yes. Individuals have the opportunity to decline to provide their personal data or to consent to particular uses of their information. ***(Explain how individuals may decline or consent to the use of their information.)***

- Not applicable. Information is not collected directly from individuals.

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

- No
- Yes *(If yes, check applicable box(es) below.)*
 - Link to FDIC Privacy Policy
 - FDIC Privacy Act Statement
 - Contractor Privacy Policy or Statement
 - No Privacy Policy has been posted
- Not applicable

SECTION V – DATA SECURITY AND ACCURACY

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

- Sandler O’Neill & Partners, LP has gone through the security review required by the FDIC’s Outsourced Information Service Provider Assessment Methodology to determine and/or verify their having appropriate physical, technical and administrative security measures to safeguard FDIC-provided PII and other sensitive data. If it has gone through the Methodology, has it been approved? NO YES

The FDIC conducts background investigations (BIs) on key Sandler personnel and other applicable personnel prior to their beginning work on the contract.

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

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

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

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

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

As necessary, Sandler's Senior Underwriter checks the data for completeness by reviewing the information, verifying whether or not certain documents or data is missing, and as feasible, updating this data when required.

Other (*Please explain.*)

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

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

Additionally, the Outsourced Information Service Provider is responsible for assuring proper use of the data. Policies and procedures have been established to delineate this

responsibility, and the vendor has designated the Mortgage Finance Principal to have overall accountability for ensuring the proper handling of data by vendor personnel who have access to the data. All vendor personnel with access to the data are responsible for protecting privacy and abiding by the terms of their FDIC Confidentiality and Non-Disclosure Agreements, as well as the vendor's corporate policies for data protection. Access to certain data may be limited, depending on the nature and type of data. (Refer to Section III of this Privacy Impact Assessment for more information on data access criteria.)

The Outsourced Provider must comply with the Incident Response and Incident Monitoring contractual requirement.

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

SECTION VI – DATA RETENTION AND DISPOSAL

16. Where will the Outsourced Service Provider store or maintain the PII data identified in question 5? Describe both electronic and physical storage repositories, as applicable.

The FDIC uploads BIS-imaged loan file data that originates from failing or failed FIs to the FDIC VDR. The uploaded BIS-imaged loan files have restricted read-only access permissions. Sandler is unable to download or store the source loan files. Additional information received via the FDIC Secure Email Service and the valuation reports generated by Sandler on behalf of the FDIC are stored on a separate, FDIC-dedicated network drive located at their New York Netapp datacenter and backups are stored on their backup datacenter in New Jersey. Both datacenters are owned and operated by Sandler O'Neill and Partners.

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

The FDIC requires valuation reports of the assigned assets to be retained on Sandler's network until the disposition strategy set forth by Sandler on the assigned assets is implemented. Sandler is required to maintain the data for three (3) years following final payment for the contract, or for any longer period required by statute or another clause in this contract. Sandler must make the materials available to the FDIC for audit, examination and reproduction, at reasonable times during the retention period. Sandler must also provide the FDIC with working space at its facilities to conduct the audit and examination.