

PRIVACY IMPACT ASSESSMENT

Shared Loss Agreement Compliance Monitoring Contractors (SLA-CMC)

May 2013

FDIC External Service

Table of Contents

[System Overview](#)
[Personally Identifiable Information \(PII\) in SLA-CMCs](#)
[Purpose & Use of Information in SLA-CMCs](#)
[Sources of Information in SLA-CMCs](#)
[Notice & Consent](#)
[Access to Data in SLA-CMCs](#)
[Data Sharing](#)
[Data Accuracy in SLA-CMCs](#)
[Data Security for SLA-CMCs](#)
[System of Records Notice \(SORN\)](#)
[Contact Us](#)

System Overview

When a financial institution fails and the FDIC is appointed as receiver, one of the FDIC's primary tasks is to dispense of the failed institution's loans and assets in a manner that maximizes their value. In order to carry out this task, the FDIC employs a Purchase and Assumption (P&A) transaction strategy with a Shared Loss Agreement ("SLA" or "shared loss"). An SLA is a contractual arrangement between the FDIC and an Acquiring Institution (AI), where the FDIC absorbs a significant portion of the loss on a specified set of assets. SLAs help maximize asset recoveries and minimize losses to the Corporation. Additionally, SLAs also reduce the FDIC's immediate cash needs, are simpler to operate and more seamless to customers of the failed institution, and move assets quickly into the privacy sector.

Under Shared Loss Agreements, the AI is required to provide financial reports on the performance of assets covered by the agreement and, as applicable, conform to loan modification programs¹ set forth by the FDIC or other governing federal agencies. Within FDIC, the Division of Resolutions and Receiverships (DRR) Risk Sharing Asset Management (RSAM) staff is responsible for managing AI compliance with the FDIC's shared-loss program. To assist with this responsibility, the FDIC/DRR utilizes the services of third-party Shared Loss Agreement (SLA) Compliance Monitoring Contractor (CMC) firms. These contracting firms currently include KPMG LLP, Signet Partners, Financial Industry Technical Services (FITS), Clayton Services LLC, Deva and Associates, Warbird (Huron Consulting Services LLC), Corvus Group, and the Watkins Consulting Group. SLA-CMCs provide risk-based² compliance monitoring of Shared Loss Agreements for commercial and other non-single family assets, as well as for single family assets, including whole loans and securities backed by single family residential loans.

The primary services that SLA-CMCs provide to the FDIC include: (1) conducting independent on-site and off-site compliance reviews to ensure AIs comply with the terms of their respective Shared Loss Agreements; (2) documenting the resolution of AI Compliance Review Findings; (3), and if requested by the FDIC, conducting loss analysis, and preparing recommendations pertaining to the suitability and level of FDIC loss reserves for the SLA transactions. As part of these activities, SLA-CMCs create and maintain hardcopy and electronic monitoring files and work papers to document the AIs' administration of covered loss share assets and loan modification denials. The files and work papers maintained by SLA-CMCs may include copies of failed institution and AI legacy loan and asset records that contain personally identifiable information (PII) about customers, borrowers, and guarantors of failed/acquiring financial institutions.

¹ AI compliance with loan modification programs is required for loss share single family (SF) assets. For more information about loan modification proposals and programs put forth by the FDIC and federal government, refer to www.FDIC.gov/loanmod/.

² Risk-based compliance monitoring focuses attention on risks inherent in Loss Share Agreements. CMCs establish specific objectives for addressing compliance risk by analyzing risk factors such as Financial Risk and Reputational Risk as it pertains to the relationship between the FDIC and AI.

Personally Identifiable Information (PII) in SLA-CMCs

SLA-CMCs create and maintain hardcopy and electronic monitoring files and work papers containing PII and sensitive information. This includes: full name, date of birth (DOB), place of birth, Social Security Number (SSN), employment status and history, mother's maiden name, home address, phone numbers (non-work), personal email addresses, financial information, driver's license information, vehicle identifiers, legal documents (i.e., divorce decree, criminal records), military status and records, as well as photographic identifiers.

Purpose & Use of Information in SLA-CMCs

SLA-CMCs use the PII specified above to review Acquiring Institutions' compliance with the terms of their respective Shared Loss Agreements. Specifically, the scope of SLA-CMC reviews includes, but is not limited to:

- Ensuring AI compliance with loss mitigation efforts;
- Ensuring AI compliance with consideration of charge-offs, foreclosure, loan restructuring, and short-sale alternatives that resulted in the least amount of loss;
- Testing the AI's policies and procedures to ensure uniform standards are being applied to both loss share and non-loss share assets;
- Reviewing internal audit reports, external independent public accountant reports, and other regulators' reports to identify potential areas of high risk associated with business and systems processes, lapses in internal controls, and weaknesses in asset recovery, workout or disposition strategies; and
- Ensuring that adequate accounting, reporting, and record-keeping systems are in place.

Sources of Information in SLA-CMCs

There are several methods for how SLA-CMCs gather PII from internal FDIC systems and applications as well as external non-FDIC systems and applications.

The first method involves acquiring institutions (AIs) adding information. AIs participating in the FDIC's shared-loss program are required to submit "certificates for payment," which are financial reports with the status of their loss-share activity, to FDIC DRR Risk Sharing Asset Management (RSAM) staff. AIs upload their certificates and relevant supporting documentation to support their claims for reimbursement to the secure FDIC Resolution Data Aggregator (RDA) system. Once uploaded into RDA, the certificates undergo a comprehensive validation process. The supporting data/schedules uploaded by the AIs may contain sensitive PII about customers, borrowers, and guarantors of failed financial institutions, such as names, home addresses, loan account numbers and balances, and SSNs. Authorized SLA-CMC staff then access RDA to review the results of the validation process and download pertinent AI certificates and supplemental data from RDA and uploads it to their secure SLA-CMC systems and/or hardcopy records in support of their compliance review activities. The data downloaded by SLA-CMC staff may include PII about borrowers/customers/guarantors of failed/Acquiring Institutions.

The second method by which SLA-CMCs gather PII data is via the FDIC Virtual Data Room (VDR). While RDA serves as the means for how AIs submit certificates, the VDR serves as the system through which AIs, SLA-CMCs, and FDIC RSAM staff upload/exchange data thereafter. AIs may upload the following to their dedicated workspace in the FDIC's secure VDR: cases/reports (i.e., reports on charge-off accounts) with documentation to support their claims for covered losses (i.e., appraisals, summary of conversations with borrowers, loan documents, etc.), as well as various documents that SLA-CMCs request to complete their compliance reviews or solve findings. The documentation provided by AIs may include borrower names, loan numbers and amounts, and home addresses, as well as Tax Identification Numbers (TINs)/SSNs. FDIC RSAM staff and/or Task Order Oversight Managers (TOOMs) may also upload advance materials and other documentation to the VDR for retrieval by SLA-CMC staff. These materials are intended to facilitate CMC compliance reviews and could include any of the documentation that an AI would add. Authorized SLA-CMC staff access the secure FDIC VDR and download the data to their secure SLA-CMC systems and hardcopy files.

Another key way that SLA-CMCs obtain PII is through their on-site compliance visitations at the AI's and their Servicers' locations. As required by the FDIC, SLA-CMCs travel to the AI (or to the AI Servicers') sites to conduct on-site compliance reviews. As part of these reviews, SLA-CMCs interview AI staff and collect and review AI certificates, schedules, and other records pertaining to the AI's administration of loss share claims and loan modification denials. This includes but is not limited to failed institution and AI legacy loan and credit files, AI policies and procedures, internal audit reports, external independent public accountant reports, etc. This information, particularly the loan files and supporting documentation for claims and loan modification denials (i.e., charge-off memos, borrower financial statements, appraisals, settlement sheets, tax, and other expense payment records, etc.) may contain sensitive information and PII about customers, borrowers, and guarantors of failed/acquiring financial institutions. During the on-site visits, SLA-CMCs securely scan/copy this AI data and upload it to their secure monitoring files and work papers (which may be in electronic and hardcopy format).

Notice & Consent

Individuals do not have the opportunity to "opt out" of providing their data or consenting to particular uses of their information. Personal information is not collected directly from individuals. PII is obtained from failed institution and assuming institution legacy loan files, and is necessary to support the conduct of SLA-CMC compliance reviews of Shared Loss Agreements on behalf of the FDIC.

Access to Data in SLA-CMCs

Authorized FDIC employees and contractors have access to the data provided to the SLA-CMCs. After the SLA-CMC conducts a compliance review of the Acquiring Institution (AI), the SLA-CMC prepares a compliance report along with supporting files and work papers (which contain PII) to the secure FDIC VDR. The report and supporting work papers are accessible via the VDR to authorized DRR Oversight Managers (Oms), TOOMs/RSAM Specialists and Technicians, and Technical Monitors

(TMs) who have responsibility for overseeing and reviewing the work of the SLA-CMC. Authorized Receivership Assistance Contract (RAC) contractors who support DRR employees may have access on an “as-needed” basis to SLA-CMC reports and work papers containing PII for purposes of helping FDIC staff manage the processing and review of this data.

Authorized SLA-CMC staff also have access to the borrower/customer/guarantor PII as part of their compliance review activities. SLA-CMCs have access to or share PII data via the FDIC Resolution Data Aggregator (RDA) system as well as the FDIC Virtual Data Room (VDR). AIs upload their required certificates and data, which may include PII, to the secure RDA. SLA-CMCs are given access to designated folders/data within RDA on a “need to know” basis in order to download the AI certificates and validation results needed to conduct their assigned compliance reviews. As previously stated, SLA-CMC staff uploads their respective compliance reports and monitoring files/work papers (which contain PII) to the secure VDR for review by authorized FDIC DRR staff and contractors.

Data Sharing

Other Systems that Share or Have Access to Data in the System:

System Name	System Description	Type of Information Processed
Resolution Data Aggregator (RDA)	Acquiring institutions (AIs) upload their required certificates and data, which may include PII, to the secure RDA. SLA-CMCs are given access to designated folders and data within RDA on a “need to know” basis in order to download the AI certificates and validation results needed to conduct their assigned compliance reviews.	Full name, DOB, place of birth, SSN, employment status and history, mother’s maiden name, home address, phone numbers (non-work), personal email addresses, financial information, driver’s license information, vehicle identifiers, legal documents, military status and records, and photographic identifiers
Virtual Data Room Secure Website Services (VDR)	SLA-CMC staff uploads their respective compliance reports and monitoring files/work papers to the secure VDR for review by authorized FDIC DRR personnel.	Full name, DOB, place of birth, SSN, employment status and history, mother’s maiden name, home address, phone numbers (non-work), personal email addresses, financial information, driver’s license information, vehicle identifiers, legal documents, military status and records, and photographic identifiers

Data Accuracy in SLA-CMCs

Data is collected directly from Acquiring Institutions (AIs) and/or from the failed institutions. As such, the FDIC and its vendors rely on the AIs and their servicers to provide accurate data. SLA-CMCs work with the FDIC to verify the integrity of the data before, in conjunction with, and after inputting it into the system or using it to support the project. As necessary, an authorized user for each respective SLA-CMC firm checks the data provided by the AI for completeness by reviewing the information, verifying whether or not certain documents or data is missing and requesting that FDIC obtain updated data from the AI when required.

Data Security for SLA-CMCs

SLA-CMCs are required to protect and dispose of all PII and sensitive business information pertaining to their compliance reviews in accordance with the privacy and information security standards outlined in their contract and Confidentiality Agreements with the FDIC. Each SLA-CMC firm takes full responsibility for the conduct of their staff to ensure the confidentiality, integrity, and availability of the sensitive information collected and maintained by their respective firms on behalf of the FDIC. In addition, each SLA-CMC firm is required to go through the security review stipulated in the FDIC's Outsourced Information Service Provider Information Service Provider Assessment Methodology to verify their having appropriate physical, technical, and administrative security measures to safeguard FDIC-provided PII and other sensitive data in their care. The FDIC performs periodic, on-site reviews of SLA-CMC firms to ensure that they are handling and safeguarding all hardcopy and electronic monitoring files, work papers, reports, and other records associated with their compliance reviews, in accordance with FDIC data privacy and records retention requirements.

FDIC background checks and security clearances are required for all SLA-CMC personnel prior to granting them access to the PII and sensitive information maintained by the FDIC. Each SLA-CMC staff member's access to the secure FDIC VDR and RDA system is subject to approval by the FDIC Oversight Manager (OM). The OM confirms that SLA-CMC personnel have obtained security clearances through FDIC's Division of Administration (DOA) Security and Emergency Preparedness Section (SEPS) prior to granting access to the VDR and RDA.

System of Records Notice (SORN)

SLA-CMCs operate under the FDIC Privacy Act SORN 30-64-0013, *Insured Financial Institution Liquidation Records*.

Contact Us

To learn more about the FDIC's Privacy Program, please visit:
<http://www.fdic.gov/about/privacy/>.

If you have a privacy-related question or request, email Privacy@fdic.gov or one of the [FDIC Privacy Program Contacts](#). You may also mail your privacy question or request to the FDIC Privacy Program at the following address: 3501 Fairfax Drive, Arlington, VA 22226.

