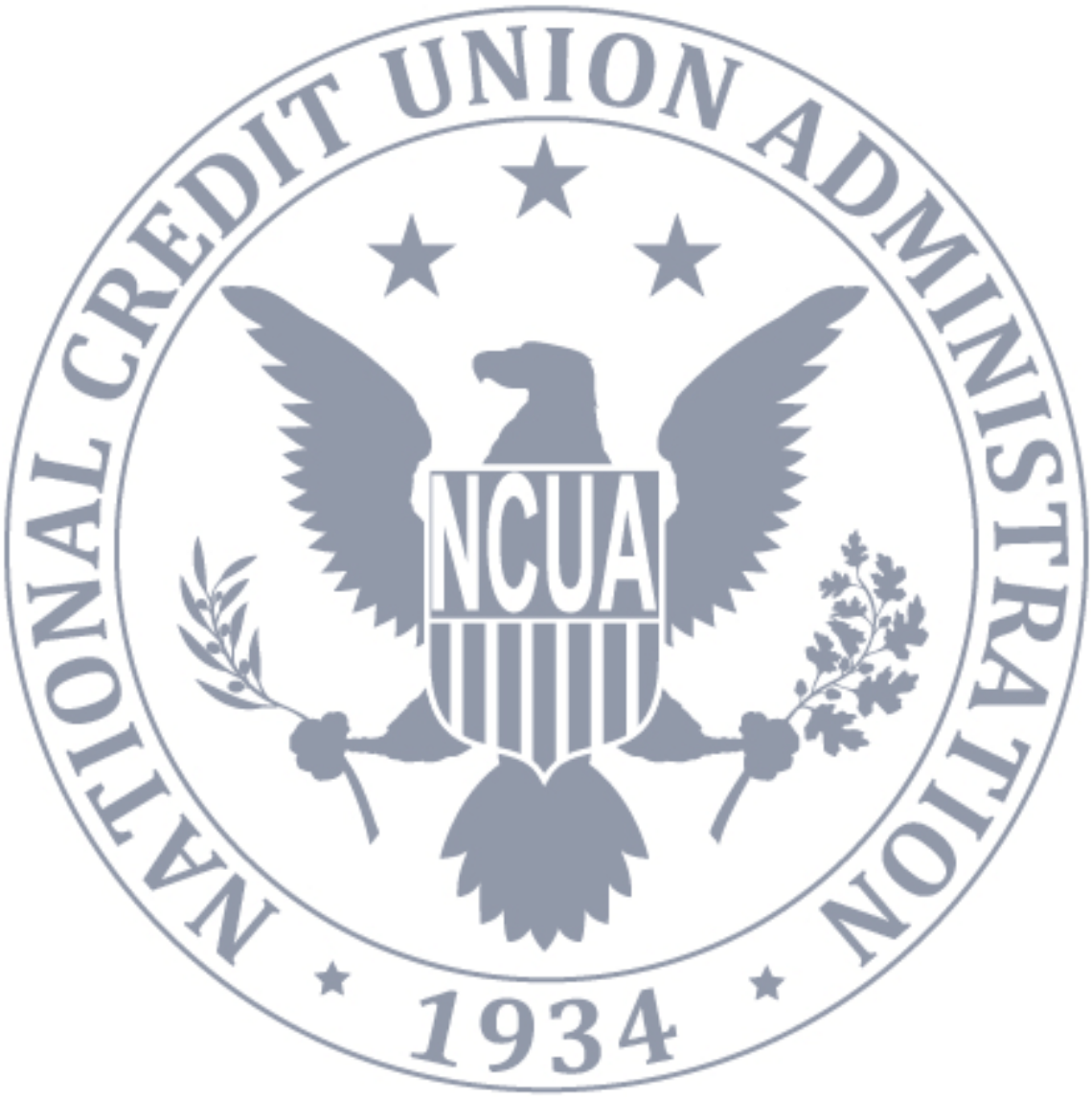
NCUA
National Credit Union Administration

Privacy Impact Assessment for ALMS, Part 1 (FISERV Advantage - AFTECH)

Fiscal Year 2018

[This page intentionally left blank]



PIA for ALMS, Part 1 (FISERV Advantage - AFTECH) • FY2018

Table of Contents

About this Document

A Privacy Impact Assessment (PIA) is an analysis of how PII is handled to ensure that handling conforms to applicable privacy requirements, determine the privacy risks associated with an information system or activity, and evaluate ways to mitigate privacy risks. A PIA is both an analysis and a formal document detailing the process and the outcome of the analysis.

Program offices and system owners are required to complete a PIA whenever they develop, procure, or use information technology to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII.[1] Completion of a PIA is a precondition for the issuance of an authorization to operate.[2]

A PIA form (and an automatic workflow and streamlined review and approval process) has been developed for consistency and ease of use. The form, and additional guidance about PIAs, is available for NCUA staff on the Privacy team's intranet site.

The Privacy team is responsible for reviewing and approving PIAs, preparing approved PIAs for publication, and otherwise managing the PIA process.

Basic Information about the System

System Name: ALMS, Part 1 (FISERV Advantage - AFTECH)

NCUA Office Owner: Asset Management and Assistance Center (AMAC)

System Manager: [redacted]

Authority

> *NCUA should only create, collect, use, process, store, maintain, disseminate, or disclose PII if it has authority to do so, and such authority should be identified in the appropriate notice.*

[1] 44 U.S.C. § 3501, note; Pub. L. 107–347, § 208(b).
[2] OMB Memorandum M-14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Act and Agency Privacy Management* (2013).

Authority for the System

12 U.S.C. § 1751 et seq.

Purpose Specification and Use Limitation

NCUA should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.

Purpose of the System

The information that is collected is used to import into the Liquidating Agent's system to facilitate the payout of insured shares to the members of liquidated credit unions. It is also used for the correspondence and collection of member loans.

Intended Use of the PII Collected

AMAC uses the information solely to assist with the analysis, administration, and servicing of loans, determining and paying share insurance, and maintaining member contact information from the liquidated credit union.

Sharing of the PII

PII in this system may be shared with:

Members of the liquidated credit union: Members are sent periodic correspondence concerning their accounts. Sensitive correspondence is sent via secure, encrypted email, USPS mail, or secure express delivery.

Assuming credit unions: When another credit union assumes the shares or purchases the loans from a liquidated credit union, NCUA will transfer the members' information to them electronically via secure, encrypted means.

Loan Servicers: Various third party loan service providers may be provided PII to service loans. Information is sent to third parties via secure, encrypted email, secure web portals, USPS mail, or secure express delivery. Information may contain a member's name and contact information (address, phone number, and email address), loan account and terms.

General Public: A listing of unclaimed shares is posted to NCUA's public-facing website. The listing includes last name, first initial, credit union name and last known city and state if available.

Department of the Treasury: In order to fulfill tax reporting requirements, information containing PII will be shared with the Internal Revenue Service, and is transmitted via USPS mail.

Minimization

NCUA should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish that purpose.

Types of PII Collected

AMAC collects PII that may include: full name; date of birth; Social Security number, employment status, history or information; mother's maiden name; home address; phone number (personal); email address (personal); employee identification number; financial information; driver's license or state identification number; vehicle identifiers; legal documents, records or notes; criminal information; and military records and/or status.

Individual Participation

NCUA should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. NCUA should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.

Opportunity for Consent

Individuals consent to their personally identifiable information being stored in this system.

Procedures to Address Individuals' Privacy Related Complaints and Inquiries

The Privacy team knows that complaints, concerns, and questions from individuals can be a valuable source of input that improves operational models, uses of technology, data collection practices, and privacy safeguards. To facilitate this type of feedback, the Privacy team has established the Privacy Complaint Process to receive and respond to complaints, concerns, and questions from individuals about NCUA's privacy practices. The process is described on NCUA's privacy website. The Privacy team appropriately records and tracks complaints, concerns, and questions to ensure prompt remediation.

Quality and Integrity

NCUA should create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.

Source of the PII

The sources of PII in this system are liquidated credit unions, Members of the liquidated credit unions, Third parties, and the U.S. Treasury.

Security

NCUA should establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.

Safeguards

Aftech access is only granted to authorized NCUA users through a secured network connection, two-factor authentication that requires PIV authentication, and a user logon access. Access by AMAC staff is role-based, related to their "need to know" in performing official duties to resolve liquidation estates.

In addition, AMAC staff are required to follow NCUA's information protection rules outlined in NCUA's Security and Privacy Awareness training that all AMAC employees must take annually, and certify that they will follow NCUA, and AMAC

Rules of Behavior for data protection.

Transparency

NCUA should be transparent about information policies and practices with respect to PII, and should provide clear and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

Applicable SORN

This system is covered by NCUA-10.

Availability of Privacy Notices

The SORN and PIA for ALMS, Part 1 (FISERV Advantage - AFTECH) are publicly available on the privacy page of NCUA's website.

Accountability

NCUA should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. NCUA should also clearly define the roles and responsibilities with respect to PII for all employees and contractors, and should provide appropriate training to all employees and contractors who have access to PII.

Compliance with the Fair Information Privacy Principles

As evidenced by this PIA (and the other information publicly available on the privacy page of NCUA's website), NCUA is committed to achieving and maintaining compliance with the Fair Information Privacy Principles.

Roles and Responsibilities of NCUA Staff

As detailed in the NCUA Computer Security Rules of Behavior, all NCUA staff are responsible for protecting PII from unauthorized exposure and for reducing the volume and types of PII necessary for program functions. Staff must protect all PII that they handle, process, compile, maintain, store, transmit, or report on in their daily work.

To protect PII, staff must use proper collection, storage, transportation, transmission, and disposal methods, must not access PII beyond what they need to complete their job duties, and must not disclose PII to unauthorized parties. Managers are also responsible for providing their subordinates with context-specific practical guidance about protecting PII.

All NCUA staff are required to review and acknowledge receipt and acceptance of the Rules of Behavior upon gaining access to NCUA's information systems and associated data.

Failure to protect PII may result in administrative sanctions, and criminal and/or civil penalties.[3]

Training

Together with the Office of Human Resources, the Privacy team ensures that new employees complete mandatory privacy training, and all existing employees and contractor employees complete privacy refresher training once every fiscal year. NCUA staff electronically certify acceptance of their privacy responsibilities as a part of annual privacy refresher training. The Privacy team keeps auditable records of completion of all mandatory trainings.

Approval

This PIA was approved by or on behalf of the Senior Agency Official for Privacy on 6/19/17.

[3] 5 U.S.C. § 552a(i)(3); NCUA Computer Security Rules of Behavior.