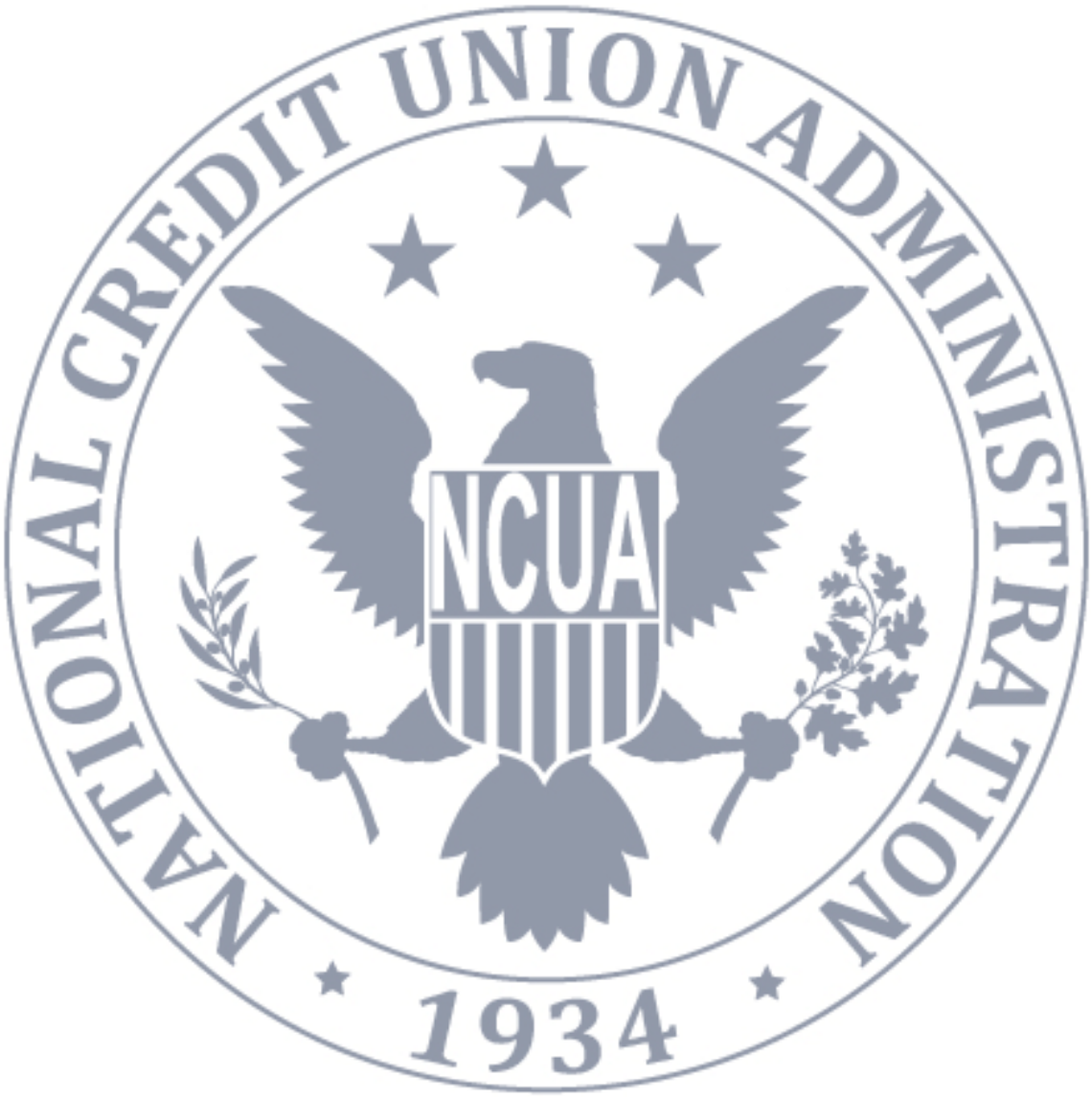
NCUA
National Credit Union Administration

Privacy Impact Assessment for NCUA Consumer Assistance Center Data Management System

Fiscal Year 2018

[This page intentionally left blank]



PIA for NCUA Consumer Assistance Center Data Management System • FY2018

Table of Contents

About this Document 2
Basic Information about the System 2
Authority 2
Purpose Specification and Use Limitation 3
Minimization 5
Individual Participation 6
Quality and Integrity 7
Security 7
Transparency 8
Accountability 8
Approval 9

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: NCUA Consumer Assistance Center Data Management System

NCUA Office Owner: OCFP

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 purpose of collecting this information is so that the NCUA CAC may address and manage consumer complaints by consumers against federally insured and state chartered credit unions. Any PII data required by the CAC, via the Salesforce system, is utilized by authorized NCUA Salesforce system users to respond to, report on, and locate submitted communications, including consumer complaints and inquiries, submitted by both individual consumers and credit union users.

Intended Use of the PII Collected

The intended use of this information is for the NCUA CAC to address and manage consumer complaints by consumers against federally insured and state chartered credit unions. Any PII data required by the CAC, via the Salesforce system, is utilized by authorized NCUA Salesforce system users to respond to, report on, and locate submitted communications, including consumer complaints and inquiries, submitted by both individual consumers and credit union users

Sharing of the PII

The PII information collected by the system is shared with credit unions and specific NCUA staff based on defined user roles.

Credit Union Access: Credit unions (external parties) have limited access to the data in the system, if registration to use the system was approved by NCUA. The purpose of this limited access is to review/respond to consumer complaints regarding the identified credit union. Credit unions may only access data in the system upon approval of their submitted portal registration request to the Office of Consumer Financial Protection, Division of Consumer Affairs.

Consumer Access: Consumers have access only to information pertaining to their own case that they have submitted via the Consumer Complaint Portal, after being registered to use the portal. Consumers register to use the system via the online Consumer Assistance Center. A consumer may only see the information they submit to their profile.

NCUA Staff Access:
Salesforce system data is protected by role-based access control limits wherein each role type defines the data an individual user may see and what actions he or she may perform. NCUA grants access to the Salesforce system based on the user roles outlined below, which are dictated by NCUA position descriptions. Only personnel who require the information in the performance of their official duties are granted access to the information. The Salesforce system is configured based on the following role types:

1. CAC manager/NCUA system administrators – These managers will have full administrative rights that include the ability to create new fields in the system, create new users, create new reports, edit any record in the system, delete data from the system, and view all data contained in the system.

2. CAC Technician– These users will have access to cases that includes the ability to view, input data, edit and update, for these cases and update the status for these records.

3. CAC Specialist– These users will be able to view, edit and update cases, input data for these cases and update the status for these records.

4. CAC Analyst– These users will be able to view, edit and update the status for record-level data initiated by a technician or specialist.

5. The Office of Consumer Financial Protection -Consumer Compliance Outreach and Policy -These users will have read-only rights for cases falling under their purview.

6. Regional DOS Director – These users will have read-only rights for cases falling under the purview of his or her region to review cases.

7. Examiners-These users will have read-only rights for cases for the purposes of pre-exam planning activities. Their access will be restricted to cases filed against those credit unions that fall under the purview of his or her region.

8. NCUA Ombudsman-These users will have read-only rights for cases to be reviewed as the NCUA Ombudsman.

Specifically, authorized NCUA staff in the central and regional offices have access to data in the system for the purposes of processing complaints, generating reports, and

conducting complaint reviews during the pre-exam planning phase of a credit union examination.

Additionally, authorized NCUA Salesforce system users, including NCUA Consumer Assistance Center personnel, based upon their official duties, will also store the necessary portion of PII in the Salesforce system cloud to perform their official work in their work-related, user profile. Use of the system in this capacity is limited to NCUA's OCFP staff members, including: technicians, specialists, analysts, program officers, and directors. Their PII includes: username, email address and telephone number (optional). These users have access to data in the system necessary for each NCUA Consumer Assistance Center employee to process information received during the course of their official duties.

Additionally, consumers have limited access to data in the system via the Consumer Complaint Portal, which is only granted via a registration process. Consumers register to use the system via the online Consumer Assistance Center.

Additionally, a contractor is responsible for configuring the Salesforce system platform. NCUA requires all contractor personnel to sign non-disclosure agreements, rules of behavior, and compliance with contract, Privacy Act and systems security requirements prior to gaining access to NCUA's network and applications.

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

The NCUA Consumer Assistance Center (CAC) collects and stores: individual names, addresses (physical and e-mail), unique identifiers (case numbers) and phone numbers of consumers who contact the CAC via written communication, telephone call, or web request when they submit an inquiry pertaining to credit union compliance or behavior, or file a formal complaint against a credit union in the Salesforce system cloud. Credit Union employees' personally identifying information, such as name, email address, employment address and phone number may also be collected and stored in this system.

The CAC, via the Salesforce system, also allows consumers and credit unions the opportunity to communicate with the CAC via a portal in the Salesforce system. To

utilize the portal, both consumer and credit union users may opt to create a unique user identification (id) and password by providing the CAC, via the Salesforce system, with PII in the form of a valid email address, physical address, name and phone number to create a log-in to check the status of, or to update, their case. The Salesforce system stores the PII information within the Salesforce system cloud. It offers both credit union and consumer users the ability to re-set their passwords by validating their accounts using a combination of name and e-mail address. For those consumers who choose not to create a unique user id and password to utilize the portal, the Salesforce system provides them the opportunity to complete the complaint, inquiry and appraisal forms, check their case status, and send the CAC email communication via the newly created "guest access" page on the Salesforce system hosted MyCreditUnion.gov landing page.

NCUA does not require PII such as social security numbers, date of birth, or other such sensitive information from the public, although individuals may sometimes provide such information. Upon receipt of any PII received electronically that is not required for the processing of a complaint, CAC staff are instructed to permanently delete the sensitive or PII information from the hard drive and network of the receiving employee. For any PII received via regular mail or fax, CAC staff are instructed to immediately destroy the sensitive or PII information by disposal in a shredder.

Individual consumers who communicate to the CAC, via the Salesforce system, are provided a unique case number. This case number is shared with the credit union personnel responsible for responding to the consumer communication forwarded to them by authorized NCUA Salesforce system users. The case number is the primary identification tool by which authorized NCUA Salesforce system users respond to, report on, and locate submitted consumer and/or credit union communications.

Additionally, when consumer or credit union Salesforce system users call into the CAC to inquire about a case, they are prompted for their individual case number. Through the individual case number, NCUA staff routes the individual to the appropriate NCUA staff member to handle the call. Accordingly, the Salesforce system's primary method of information retrieval is the assigned unique identifier number, and not PII. Again, PII is used to locate consumer and credit union records only after the Salesforce system has attempted to locate the record utilizing the assigned unique case number. In addition, consumers have the option of using a guest account, which still requires the assignment of a unique identifier number to his/her case.

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 data is collected from either individual consumers or credit unions against whom complaints are submitted. The information is submitted electronically or by hard copy mail, fax, or through telephone calls to the CAC through our Salesforce telephony integration with NCUA's call vendor, Genesys. When consumers call the CAC, they are asked to verify information to ensure the identity of the consumer. Such information may include: name, address or case number which is entered by NCUA into the Salesforce System. It should be noted that the chosen NCUA telephony technology vendor, Genesys, does not store PII data. It simply supports the Salesforce system through telephony technology.

The CAC, via the Salesforce system, receives electronic referrals of consumer complaint information, possibly containing PII, from various other federal or state government agencies, which include, but is not limited to: Consumer Financial Protection Bureau (CFPB), Federal Deposit Insurance Corporation (FDIC), Federal

Reserve Board (FRB) and the Office of the Comptroller of Currency (OCC). The data received from these organizations is comprised of consumer complaints that may fall within NCUA purview. Accordingly, received complaints that fall within CAC purview are opened and processed as other consumer communication outlined above. No third party sources will provide data to the system.

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

Information in the system is safeguarded in accordance with the applicable laws, rules and policies governing the operation of federal information systems.

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-12.

Availability of Privacy Notices

The SORN and PIA for the NCUA Consumer Assistance Center Data Management System 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.

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

Approval

This PIA was approved by or on behalf of the Senior Agency Official for Privacy on 4/3/18.