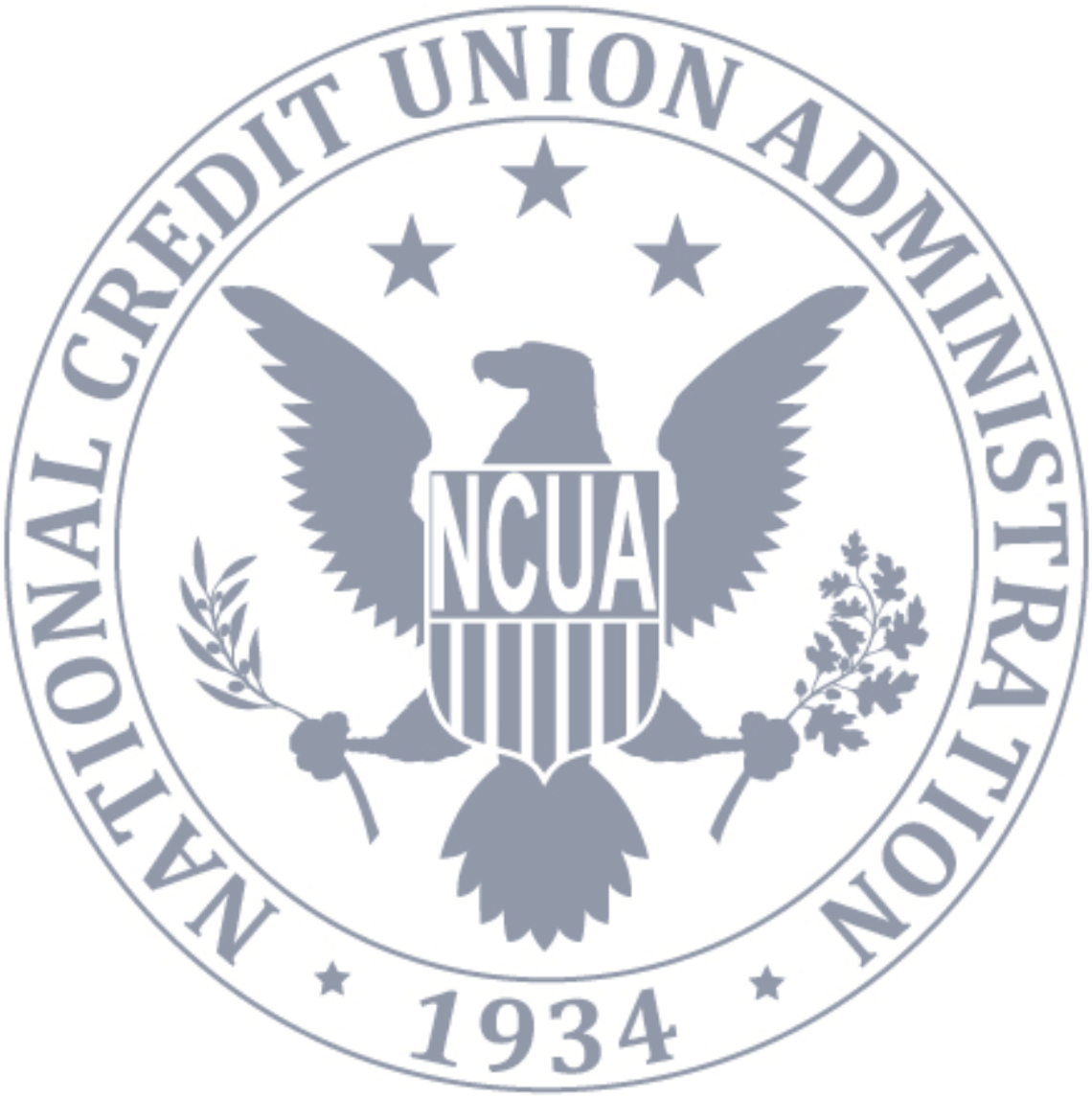
NCUA
National Credit Union Administration

Privacy Impact Assessment for Genesys-Salesforce Consumer Assistance Center

Fiscal Year 2018

[This page intentionally left blank]



PIA for Genesys-Salesforce Consumer Assistance Center • 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: Genesys-Salesforce Consumer Assistance Center

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 Genesys Telecommunications system is a telephony subsystem integrated into NCUA Consumer Assistance Center Salesforce platform, for the purpose of making and receiving phone calls to and from the public through the Consumer Assistance Center (CAC). The PII collected depends on the nature of the call. All activity on the Genesys platform-both outbound and inbound-is recorded and stored on the Genesys platform for periodic quality control or emergency management purposes.

Intended Use of the PII Collected

PII collected is results from the call recording function. Only when necessary, phone calls recordings in the form of .wav files are pulled from the Genesys platform cloud for review to ensure staff compliance with established CAC customer service policies, and to occasionally review calls involving sensitive topics of a threatening nature. No live call data recordings are stored on the Salesforce platform, other than the notes regarding the customer interaction that are manually recorded by the CAC staff. Callers that choose to leave a voicemail trigger the voicemail function from the Genesys platform. This function allows a consumer to leave a voicemail for a CAC staff member, and through the integration with the Salesforce platform the content of the .wav filed generated from the call is transcribed into written text, and stored into the associated Salesforce case/Privacy Act system for CAC staff review and response.

Any PII data received by the CAC, via Genesys, will be utilized by CAC staff during their daily required duties to respond to, report and locate submitted communications from the general public, including consumers.

Sharing of the PII

Any information collected in the Genesys platform may only be shared outside of the Consumer Assistance Center with other authorized NCUA employees with an official need to know to perform their official duties, or law enforcement bodies for the purpose of investigating threatening communications received in the Consumer Assistance Center.

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 potential PII includes:

- NCUA employees - First/last name, username, and password.
- General Public (e.g., the callers) – PII can vary. PII may include: individual names, addresses, account numbers, phone numbers, and case/complaint numbers.

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

Due to the nature of this system, there is not an opportunity to ask individuals to consent.

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 the general public (consumers). The information is collected through telephone communications to and from the Consumer Assistance Center via the Genesys platform. The call data is stored on the Genesys platform.

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

By the nature and purpose of the Genesys sub-system, individual callers (consumers/members of the public) voluntarily contact the CAC. Each call is notified at the beginning of the call that it is recorded only for customer service purposes, and in the event of an emergency. In addition, the Consumer Assistance Center does not require a caller to provide specific PII when handling telephone communications involving matters not pertaining to a specific consumer complaint. If the individual caller requests the details of a submitted complaint, for security and privacy purposes,

the CAC staff must first verify the individual's identity/contact information to confirm that it is the caller's case to which s/he would be allowed to be updated on the case.

The Genesys Telecommunications system is compliant to PCI DSS Requirements. It meets HIPPA, ISO 27001, and SOC II standards.:

- Access to data is restricted only to authorized Office of Consumer Financial Protection and Access (OFCPA) employees by business function, and based upon their roles and need to know to perform their official duties.
- A two-factor identification and authentication access to the system is used.
- OFCPA employees are only able to access the CAC cases assigned to them.
- Access to the network, system and data is continuously tracked and monitored.

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 Genesys-Salesforce Consumer Assistance Center 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 7/17/17.