Customer Assistance Group (CAG) Remedy

Privacy Impact Assessment (PIA)

Version 2.2

September 5, 2012

Prepared by:

Security and Compliance Services

Comptroller of the Currency
Administrator of National Banks

US Department of the Treasury

Purpose

The Privacy Impact Assessment (PIA) is completed as a mandatory step in the certification and accreditation of IT systems, applications, and projects, that collect, process, store, and disseminate Personally Identifiable Information (PII). The PIA examines the ways in which PII data are managed and protected by the target of evaluation.

Do not include any Sensitive Information in the PIA. When finalized, the PIA will be a publicly-accessible document posted to the OCC public-facing website.

Questions regarding this PIA template should be directed to the OCC Privacy Act Officer for response.

NOTE

This document was prepared in support of the system's Certification and Accreditation effort. The document was developed in accordance with, or following the guidance contained in, the following:

- *The Privacy Act of 1974* (Public Law 92-132, 5 U.S. C. 552a).
- *Federal Information Security Management Act of 2002* (Title III of P.L. 107-347).
- Section 208 of the *E-Government Act of 2002* (Public Law 107-347, 44 U.S.C. Ch 36), April 17, 2003.
- Office of Management and Budget (OMB) Memorandum M-03-18, *Implementation Guidance for the E-Government Act of 2002*, August 1, 2003.
- OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 26, 2003.
- OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information*, May 22, 2006.
- OMB Circular No. A-130**,** Revised, (Transmittal Memorandum No. 4)**:** *Management of Federal Information Resources*, 28 November 2000.
- Computer Matching and Privacy Act of 1988 (Public Law 100-503).
- Department of the Treasury Publication, TD P 25-05, *Privacy Impact Analysis Manual*, dated July 2006

DOCUMENT CHANGE CONTROL

VERSION	DATE	SUMMARY OF CHANGES	NAME
2.1	8/22/12	Reviewed and Updated	K. Kaplan

Table of Contents

Page

1. SYSTEM IDENTIFICATION 4

1.1 NAME OF SYSTEM, PROJECT, OR PROGRAM: 4
1.2 RESPONSIBLE ORGANIZATION 4
1.3 INFORMATION CONTACT(S) 4
1.4 SECURITY CATEGORIZATION 4
1.5 SYSTEM OPERATIONAL STATUS 5
1.6 GENERAL DESCRIPTION/PURPOSE 5
1.7 FUTURE CHANGES TO CAG REMEDY 6
1.8 SYSTEM INTERCONNECTION/INFORMATION SHARING 6

2. PRIVACY IMPACT ASSESSMENT 6

2.1 PRIVACY ASSESSMENT 6
2.2 DATA IN THE SYSTEM/APPLICATION 7
2.3 SYSTEM OF RECORDS (SOR) NOTICE 10
2.4 CERTIFICATION AND ACCREDITATION 10

PRIVACY IMPACT ASSESSMENT

1. SYSTEM IDENTIFICATION

1.1 Name of System, Project, or Program:

Customer Assistance Group (CAG) Remedy

1.2 Responsible Organization

OCC Office of the Ombudsman, 1301 McKinney Street, Houston, TX, 77010

1.3 Information Contact(s)

Key System Contacts (include name, phone, and email):

See PTA (Privacy Threshold Analysis) document.

1.4 Security Categorization

The system was assessed in its Security Categorization Report (SCR) as **MODERATE** under guidance contained in Federal Information Processing Standards (FIPS) Publication (PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*, December 2003, as follows:

Information Type	Confidentiality	Integrity	Availability
Corrective Action	Low	Low	Low
Program Evaluation	Low	Low	Low
Program Monitoring	Low	Low	Low
Budget Execution	Low	Low	Low
Customer Service	Low	Low	Low
Official Information Dissemination	Low	Low	Low

Information Type	Confidentiality	Integrity	Availability
Product Outreach	Low	Low	Low
Income	Moderate	Moderate	Moderate
Personal Identity and Authentication	Moderate	Moderate	Moderate
IT Security	Low	Moderate	Low
Financial Sector Oversight	Moderate	Low	Low
Legal Investigation	Moderate	Moderate	Moderate
Resolution Facilitation	Moderate	Low	Low
General Purpose Data & Statistics	Low	Low	Low
Advising & Consulting	Low	Low	Low
Overall Per Category	**Moderate**	**Moderate**	**Moderate**
System Overall	**MODERATE**		

1.5 System Operational Status

The System is currently **operational.**

1.6 General Description/Purpose

The Customer Assistance Group (CAG) assists consumers who have questions or complaints about national banks and federal savings associations (thrifts) and their operating subsidiaries. CAG provides service to three constituent groups:

- Customers of national banks and federal savings associations (thrift) and their subsidiaries – by providing a venue to resolve complaints.
- OCC bank and federal savings associations (thrift) supervision – by alerting supervisory staff of emerging problems that may potentially result in the development of policy guidance or enforcement action.
- National bank and federal savings associations (thrift) management – by providing a comprehensive analysis of complaint volumes and trend.

The CAG Remedy application is used by CAG Specialists, Tier One Customer Service Representatives, and the E-Business unit within the OCC.

The CAG Remedy application is used to:

- store information related to Consumer complaints involving financial institutions and provide access to documents related to consumer complaints
- store institutional data
- apply workflow rules to ensure prompt handling of Consumer complaints
- provide the data used for reporting purposes
- provide the data used by banks and federal savings associations (thrift) to resolve Consumer complaints
- archive information related to cases
- receive zip code data imports

1.7 Future Changes to CAG Remedy

None

1.8 System Interconnection/Information Sharing

CAG Remedy does not have interconnections to any external information systems.

2. PRIVACY IMPACT ASSESSMENT

2.1 Privacy Assessment

The following paragraphs detail the Privacy Assessment applicable to CAG Remedy.

2.1.1 Does this system collect any personal information in identifiable form about individuals?

Yes ☑ No ☐

2.1.2 Does the public have access to the system?

Yes ☐ No ☑

2.1.3 Has a PIA been completed in the past?

Yes ☑ No ☐

2.1.4 Has the existing PIA been reviewed within the last year?

Yes ☑ No ☐ N/A ☐

2.1.5 Have there been any changes to the system since the last PIA was performed?

Yes ☐ No ☑ N/A ☐

2.2 Data in the System/Application

2.2.1 What elements of PII are collected and maintained by the system?

The CAG Remedy Case Management system contains information related to complaints filed against financial institutions by consumers. Each case may potentially contain the following personally identifiable information provided by the consumer: name, address telephone, bank and federal savings associations (thrift) account numbers, and social security numbers. If the consumer has an attorney or other representative, a complaint could also include information about that representative, e.g., name, title, telephone number.

2.2.2 Why is the information is being collected?

The OCC and other financial regulatory agencies are required by the following laws and executive orders to respond to consumer complaints and to integrate analyses of complaints into the development of policy.

- **The Magnuson - Moss Warranty -- Federal Trade Commission Improvement Act of 1975**, requires the Office of the Comptroller of the Currency, the Federal Reserve Board, the Federal Deposit Insurance Corporation and the National Credit Union Administration to have a Consumer Affairs Division to receive and take appropriate action on complaints with respect to unfair or deceptive practices by institutions subject to their jurisdiction.
  See 15 USC 57a(f)(1).

- **Executive Order 12160, dated September 26, 1979**, established a consumer affairs council and required federal agencies to review and revise operating procedures so that consumer needs and interests would be adequately considered and addressed. In establishing the consumer programs, the agencies were required to establish procedures for systematically logging, investigating, and responding to consumer complaints, and for integrating analyses of complaints into the development of policy.

- **Executive Order 12862, dated September 11, 1993**, requires all federal agencies that provide direct services to the public to determine the kind and level of services that satisfy customers; establish customer service standards; provide easily accessible means to address customer complaints; and measure performance against the best in the business.

CAG Remedy collects the information types listed in 2.2.1 to support the processing of consumer complaints.

2.2.3 What are the sources of the information in the system?

The sources of PII information in CAG are the complaint filing options listed in 2.2.1.

2.2.4 How will the data collected from sources other than Federal agency records or the individual be verified for accuracy?

CAG requires consumers who use the Ombudsman's online consumer complaint form to file their complaints to certify the accuracy of their input as part of the process of completing the form. The referenced institutions also validate this data against their records as consumer complaints are transmitted to them for their response. Should an institution not have a record of the consumer filing a particular complaint, the institution can request that the OCC's Customer Assistance Group research and validate consumer information. In such instances, the OCC prompts the consumer via letter or email to contact the OCC's 1-800 customer service line for additional information.

2.2.5 Who will have access to the data and how is access determined?

Customer Assistance Group managers use the ITS Remedy system to authorize access to CAG for their staff, and the IT Customer Support technical personnel technically provides that access. Access levels are allocated on a need to know and consistent with least privilege. User accounts are routinely audited to ensure access levels are appropriate. Processes are consistent with agency direction on appropriate access controls for systems containing SBU.

2.2.5 Describe the administrative and technological controls that are in place or that are planned to secure the information being collected.

All management, operational, and technical controls in place for CAG Remedy are documented in a system security plan, developed and tested according to direction for the protection of moderate security systems published by the National Institute of Standards and Technology (NIST) special publication series, especially NIST Special Publication (SP) 800-18, NIST SP 800-53, and NIST SP 800-53a

2.2.6 What opportunities will individuals have (if any) to decline to provide information or to consent to particular uses of the information?

Consumers voluntarily supply their PII as a function of initiating a complaint against their financial institution. The online complaint form typically used by consumers to initiate complaints contains the following privacy statement:

PRIVACY ACT STATEMENT
The solicitation and collection of this information is authorized by 15 U.S.C. - 57a(f) and 12 U.S.C. 1 et seq. The information is solicited to provide the Office of the Comptroller of the Currency (OCC) with data that is necessary and useful in reviewing requests received from individuals for assistance in their interactions with national banks and federal savings associations (thrift). The provision of requested information is voluntary. However, without such information, the ability to complete a review or to provide requested assistance may be hindered. It is intended that the information obtained through this solicitation will be used within the OCC and provided to the national bank and federal savings associations (thrift) that is the subject of the complaint or inquiry. Additional disclosures of such information may be made to: (1) other third parties when required or authorized by statue or when necessary in order to obtain additional information relating to the complaint or inquiry; (2) other governmental, self-regulatory, or professional organizations having: (a) jurisdiction over the subject matter or the complaint or inquiry; (b) jurisdiction over the entity that is the subject of the complaint or inquiry; or (c) whenever such information is relevant to a known or suspected violation of law or licensing standard for which another organization has jurisdiction; (3) the Department of Justice, a court, an adjudicative body, a party in litigation, or a witness when relevant and necessary to a legal or administrative proceeding; (4) a Congressional office when the information is relevant to an inquiry initiated on behalf of its provider; (5) Other governmental or tribal organizations with which an individual has communicated regarding a complaint or inquiry about an OCC-regulated entity; (6) OCC contractors or agents when access to such information in necessary; and (7) other third parties when required or authorized by statute.

2.2.7 What is the life expectancy of the data and how will it be disposed of when it is no longer needed?

The current life expectancy of the data is the life of the system. Disposition will be managed consistent with IAW federal regulations for financial information, and in keeping with OCC Records Management policy, the Ombudsman's file plan, and NARA regulation.

2.2.8 Is the system owned, operated, and maintained by a contractor?

Yes ☐ No ☑

2.3 System of Records (SOR) Notice

Does the collection of this information require a new system of records under the Privacy Act (5 U.S.C. § 552a) or an alteration to an existing system of records?

Yes ☐ No ☑

2.4 Certification and Accreditation

Has the system been certified and accredited within the last three years?

Yes ☑ No ☐

Date ATO granted: October 2007, to be renewed October 2010