Privacy Impact Assessment
of the
Consumer Complaint and Inquiry Systems

Program or application name:

Consumer Complaint and Inquiry Systems (CCIS)

Contact information.

CCIS is maintained by the Board's Division of Consumer and Community Affairs (DCCA) and the Federal Reserve Bank of Kansas City.

System Owner:	Yvonne Cooper
Title:	Manager, Consumer Complaints
Organization:	Division of Consumer and Community Affairs
Address:	20th and C Streets, N.W. Washington, D.C. 20551
Telephone:	(202) 452-2633

Summary description of the program or application:

CCIS supports the Federal Reserve System's business processes for receiving, responding, monitoring and reporting consumer complaints and inquiries that are filed against state member banks and other financial institutions supervised by the Board.

CCIS includes two components: (1) the Complaint Analysis Evaluation System and Reports (Web CAESAR), which was approved in March 2006; and (2) the new Federal Reserve Consumer Help (FRCH) website. Consumer complaints and inquiries are received directly by the Federal Reserve System (FRS) via U.S. mail, telephone, fax, e-mail, and the Internet through the FRCH website. The information is then input and stored in Web CAESAR.

1. The information concerning individuals that is being collected and/or maintained.

Any contact information provided by the consumer, such as:

a. Name
b. Home address
c. Home, work, and/or cellular telephone and facsimile numbers
d. E-mail address

Information about the nature of the complaint or inquiry as provided by the consumer, such as:

a. Consumer's description of the complaint and inquiry
b. Name of the financial institution involved, if any
c. Account/Product Type
d. Institution address
e. Institution e-mail address
f. Institution telephone number
g. Additional contact or location information about the institution

2. Source(s) of each category of information listed in item 1.**

The only source of information will be the individuals who file a complaint or inquiry about an institution.

3. Purposes for which the information is being collected.

Individual information collected and maintained in CCIS relates to the Board's exercise of its statutory, regulatory and supervisory authority pursuant to, but not limited to, the Federal Reserve Act (12 U.S.C. §§ 221 *et seq.*), the consumer protection laws regarding practices by banks and other financial institutions supervised and regulated by the Board, including the Federal Trade Commission Act (15 U.S.C. § 57a(f)), and the Board's Regulations, 12 C.F.R. §§ 201 *et seq.*

4. Who will have access to the information.

For the most part, access to data by a user within the Federal Reserve is limited to authorized employees within the Federal Reserve who have a need

for the information for official business purposes. The information may also be shared with a Board-regulated entity that is the subject of a complaint or inquiry and third parties to the extent necessary to obtain information that is relevant to the resolution of a complaint or inquiry. In addition, the information may also be disclosed for enforcement, statutory and regulatory purposes; to another agency or a Federal Reserve Bank, to a Member of Congress; to the Department of Justice, a court, an adjudicative body or administrative tribunal, or a party in litigation; to contractors, agents, and others; and persons who are reasonably necessary to assist in connection with the Board's efforts to respond to the suspected or confirmed compromise of security or confidentiality and prevent, minimize, or remedy such harm; to appropriate federal, state, local, or foreign agencies where disclosure is reasonably necessary to determine whether an individual intending to visit the Board poses a security risk; or to other agencies, entities, and persons reasonably necessary to assist the Board's efforts to respond to a suspected or confirmed compromise of security or confidentiality to prevent, minimize or remedy such harm.

5. Whether the individuals to whom the information pertains have an opportunity to decline to provide the information or to consent to particular uses of the information (other than required or authorized uses).

Individuals are not required to submit any information. Moreover, once an individual has submitted information, he or she may withdraw his or her complaint or inquiry by written request at any time. However, if an individual fails to submit information or if an individual withdraws his or her complaint or inquiry, the Board will cease its investigation of/response to the complaint or inquiry.

6. Procedure(s) for ensuring that the information maintained is accurate, complete, and up-to-date.

Once a record is created in Web CAESAR, business and technical requirements ensure that the user captures all data occurrences and data elements for tracking and reporting data. Edit checks for the system ensure that data are entered and reported correctly. If any technical discrepancy is detected, it is reported to the IS Web CAESAR Administrator, who will follow up on the matter until it is resolved. Both

Board and FRCH staff have established quality assurance controls for the data contained in Web CAESAR.

7. The length of time the data will be retained, and how will it be purged.

In accordance with the Board's record retention policy, the complaint data is retained for five years after a complaint or inquiry is closed. Data that is maintained in electronic form in Web CAESAR that has reached the retention period is purged annually. Data that is maintained in paper form at either the Board or the Federal Reserve Bank of Kansas City is destroyed by shredding.

8. The administrative and technological procedures used to secure the information against unauthorized access.

The FRCH website is secured by technological controls that validate all input and servers that are protected through an application that analyzes traffic patterns to prevent malicious actions. Access to FRCH is limited to authorized Federal Reserve staff.

There are three user access levels (administrator, read and write, and read-only) in Web CAESAR to secure information against unauthorized access. Database access is limited to authorized Board and Reserve Bank Web CAESAR Administrators and IT Developers (on as needed basis). Access is given to users only after the Board IS Web CAESAR Administrator receives an electronic e-mail and a Web CAESAR "Acquiring Access" form from a Board or Reserve Bank manager or officer in charge of consumer affairs who approves a user's need for access. Authorized users are authenticated through the Board's or Reserve Bank's internal network system.

According to the FISMA requirements, controls are built into Web CAESAR to automatically deactivate the users who do not log into the system for 180 days or more.

The Board IS Web CAESAR Administrator performs an annual verification process to ensure that all Board, FRCH and Reserve Bank Web CAESAR Data Administrators adhere to the Board's security procedures for maintaining and updating Web CAESAR users.

9. Whether a new system of records under the Privacy Act should be created. (If the data is retrieved by name, unique number, or other identifier assigned to an individual, then a Privacy Act system of records may be created).

CCIS is covered under a Privacy Act System of Records notice, entitled "Consumer Complaint Information System" (BGFRS-18).

Reviewed:

(signed) Maureen Hannan	10/08/08
Chief Information Officer	Date
(signed) Charles S. Struckmeyer	10/07/08
Chief Privacy Officer	Date