Privacy Impact Assessment
of
Automated Loan Examination Review Tool

Program or application name:

Automated Loan Examination Review Tool (ALERT)

System Owner:

Board of Governors of the Federal Reserve System's ("Board") Division of Banking Supervision and Regulation (BS&R)

Contact information:

System Owner:	Sabeth Siddique, Assistant Director
Organization:	Division of Banking Supervision and Regulation
Address:	20th and C Streets, N.W. Washington, DC 20551
Telephone:	(202) 452-3861
IT System Manager:	Robert Ashman, Assistant Director
Organization:	Division of Banking Supervision and Regulation
Address:	20th and C Streets, N.W. Washington, DC 20551
Telephone:	(202) 452-3528

Summary description of the program and application:

ALERT is an examination tool developed to facilitate loan reviews of regulated financial institutions by examiners conducting safety and soundness examinations. The program enables examiners to access electronic loan data provided by banks via e-mail, diskette, or compact disk. In addition to printing the loan data from electronic media, the program provides examiners with an analytical tool for assessing risk in bank loan

portfolios. In particular, the application is used to evaluate compliance with loan concentration limits on bank loans to individual borrowers. ALERT is used by the Board, the Federal Deposit Insurance Corporation (FDIC), and most state bank regulatory agencies.

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

ALERT is not designed to capture personal information; however, certain categories of personal information are maintained, either directly or indirectly, as part of the examination process of collecting, aggregating, and analyzing loan data for a regulated financial institution during the course of the examination or continuous supervision process. The following fields in ALERT may contain personally identifiable information about individuals:

a. loan customer name;
b. address;
c. social security number;
d. taxpayer identification number;
e. loan account number;
f. loan officer name;
g. loan officer number;
h. loan balances, interest rates and payment information; and
i. non-public confidential bank loan classifications.

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

The identifiable information listed in item 1 is generally obtained by the Federal Reserve from regulated financial institutions through the examination or continuous supervision process. The source of the information in the system is an electronic file extracted from the subject bank's loan accounting system.

3. Purposes for which the information is being collected.

ALERT supports the Board's statutory responsibility to evaluate the overall credit risk and, consequently, the safety and soundness of the financial institutions that it regulates. As part of the supervisory process, Federal Reserve staff review loans made by banks to determine whether a bank's loan portfolio is financially sound, within legal guidelines, will not have a

significant impact on capital, and is not overly concentrated with particular borrowers. Federal Reserve examiners accomplish these purposes primarily by collecting and analyzing aggregate, not individual, loan data. Generally, loan data is selected, based on examiner parameters, and results of analyses of these loans are aggregated into portfolio level evaluations of loan asset quality, which are then used by Federal Reserve staff to evaluate the credit risk of supervised financial institutions. These data also permit Federal Reserve staff to evaluate bank performance relative to institutional peers.

Certain of the loan data may reference information about individuals; however, this information is primarily used to support the aggregated data analysis of a regulated financial institution's loan portfolio, rather than the analysis of individual loans. Analysis of individual loans may occur in instances where Federal Reserve staff has a business need to evaluate issues relating to, among others, individual loan concentrations, improper insider lending, fraud or suspicious activities identified during the course of the examination or continuous supervision process.

4. Who will have access to the information.

Authorized employees within the Federal Reserve are provided with access to identifiable information in ALERT on a "need to know" basis, that is, when the information is required for official business purposes. More specifically, access to the information in ALERT is generally restricted to members of the bank examination team assigned to the particular financial institution, and their supervisors and managers. However, information in ALERT is also shared within the Federal Reserve to facilitate other necessary supervisory and regulatory functions. Care is taken to ensure that only those employees who are authorized and have a need for the information for official business purposes have access to that information.

In addition, data may be shared as needed for the conduct of joint supervisory initiatives with the staff of other bank regulatory agencies, including the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, and state banking regulators pursuant to explicit information sharing agreements that require the implementation of access restrictions and security safeguards.

The information maintained in ALERT is designated as confidential supervisory information and access cannot be granted to the public;

however, under the Freedom of Information Act individual citizens may request access to ALERT information related to themselves. The information maintained in ALERT may also be used as follows:

A. Disclosure for Enforcement, Statutory and Regulatory Purposes. Information may be disclosed to the appropriate federal, state, local, foreign, or self-regulatory organization or agency responsible for investigating, prosecuting, enforcing, implementing, issuing, or carrying out a statute, rule, regulation, order, policy, or license if the information is relevant to a potential violation of civil or criminal law, rule, regulation, order, policy or license within the jurisdiction of the receiving entity.

B. Disclosure to a Member of Congress. Information may be disclosed to a congressional office in response to an inquiry from the congressional office made at the request of the individual to whom the record pertains.

C. Disclosure to the Department of Justice, a Court, an Adjudicative Body or Administrative Tribunal, or a Party in Litigation. Information may be disclosed to the Department of Justice, a court, an adjudicative body or administrative tribunal, a party in litigation, or a witness if the Board determines that the information is relevant and necessary to the proceeding and that such disclosure is compatible with the purpose for which the records were collected.

D. Disclosure to Contractors, Agents, and Others. Information may be disclosed to contractors, agents, or others performing work on a contract, service, cooperative agreement, job, or other activity for the Board and who have a need to access the information in the performance of their duties or activities for the Board.

E. Disclosure Where Security or Confidentiality Has Been Compromised. Information may be disclosed when (1) it is suspected or confirmed that the security or confidentiality of information has been compromised; (2) the Board has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or

integrity of this IT system or other IT systems or programs (whether maintained by the Board or another agency or entity) that rely upon the compromised information; and (3) the disclosure is made to such agencies, entities, and persons who are reasonably necessary to assist in connection with the Board's efforts to respond to the suspected or confirmed compromise and 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 do not have an opportunity to decline to provide the information or consent to particular uses of the information collected and maintained in ALERT. The information concerning individuals is collected directly from the financial institution, rather than from the individual to whom it may pertain, during the bank examination or continuous supervision process pursuant to the institution's statutory obligation to provide any and all financial records to its federal regulator. The information is acquired by the financial institution from its customers as a routine business activity.

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

All identifiable information collected by ALERT is obtained directly from the financial institution during the course of the bank examination process. The examiner-in-charge, or a designee, is responsible for ensuring the accuracy and completeness of the information acquired from the financial institution and processed by ALERT, to the extent possible. The EIC assigns the electronic loan trial balance file to an individual examiner whose responsibility is to ensure the file is properly imported, reconciled against separately provided documents and processed correctly by comparing and/or sampling of the data. Additionally, paper records of reconcilement are obtained from the financial institution to validate the electronic data contained in ALERT. In some instances, staff receives loan data from financial institutions in alternate formats. Staff may update the ALERT database with this data in order to include this information in the evaluation of loan asset quality. In addition, staff may correct typographical errors that would otherwise result in misreporting of data.

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

Records maintained in ALERT are typically maintained for three years; however, in the event of a supervisory or enforcement action initiated by the Board of Governors, information may be maintained for three years after termination of such supervisory or enforcement action. In some cases, aggregate or summary data may be held for longer periods to support business cycle analysis. Paper documents are destroyed by shredding. Electronic information is destroyed by deleting information from the appropriate data base(s).

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

The Federal Reserve uses a combination of methods to secure the information contained in ALERT. Federal Reserve offices are restricted-access facilities, and Federal Reserve information stored at financial institutions is secured by Federal Reserve-owned devices, such as locks. Electronic information is stored in an encrypted format on access-controlled servers and workstations. Electronic and print copies of ALERT data developed during the course of an examination are shared outside of the examination team only with Federal Reserve supervisory staff requiring access to that information to conduct their job functions. Information security configurations for electronic databases, application systems, procedures, and examination documentation are periodically reviewed by the Information Security Officers at the Reserve Banks and the Board of Governors to ensure ongoing compliance with the requirements defined in the Federal Reserve's Information Security Manual.

9. Whether a new system of records under the Privacy Act will 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).

ALERT does not require the publication of a system of records under the Privacy Act since ALERT is indexed by financial institution name, not by reference to an individual's name or other personal identifier. While

identifiable information may subsequently be retrieved by reference to an individual's name or other personal identifier in connection with an examination or continuous supervision of a particular financial institution, it cannot be independently retrieved without reference to financial institution name.

Reviewed:

(signed) Elaine Boutilier	11/20/2007
Chief Privacy Officer	Date
(signed) Maureen Hannan	12/03/2007
Chief Information Officer	Date