payments electronically, including, but not limited to, processing direct mail or performing other marketing functions; investigating and rectifying possible erroneous information; and creating and reviewing statistics to improve the quality of services provided.

(4) Federal agencies, their agents and contractors for the purposes of implementing and studying options for encouraging current and prospective Federal payment recipients to receive their Federal payments electronically.

(5) Representatives of the National Archives and Records Administration (NARA) who are conducting records management inspections under authority of 44 U.S.C. 2904 and 2906.

(6) Appropriate agencies, entities, and persons when (a) FMS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (b) FMS 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 system or other systems or programs (whether maintained by FMS or another agency or entity) that rely upon the compromised information; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with FMS’s efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:

STORAGE:
Records are maintained in paper and electronic media.

RETRIEVABILITY:
Records are retrieved by name, address, or other alpha/numeric identifying information.

SAFEGUARDS:
All official access to the system of records is on a need-to-know basis only, as authorized by a business line manager at FMS or FMS’s fiscal or financial agent. Procedural and physical safeguards, such as personal accountability, audit logs, and specialized communications security, are utilized. Each user of computer systems containing records has individual passwords (as opposed to group passwords) for which he or she is responsible. Thus, a security manager can identify access to the records by user. Access to computerized records is limited, through use of access codes, encryption techniques, and/or other internal mechanisms, to those whose official duties require access. Storage facilities are secured by various means such as security guards, badge access, and locked doors with key entry.

RECORD SOURCE CATEGORIES:
Information in this system is provided by commercial database providers based on publicly available information.

CONTESTING RECORD PROCEDURES:
See “Record access procedures” above.

DEPARTMENT OF THE TREASURY
Office of Thrift Supervision


SI Financial Group, Inc., Willimantic, CT; Approval of Conversion Application

Notice is hereby given that on November 10, 2010, the Office of Thrift Supervision approved the application of SI Bancorp, MHC, Willimantic, Connecticut, the federal mutual holding company for the Savings Institute Bank and Trust Company, Willimantic, Connecticut, to convert to the stock form of organization. Copies of the application are available for inspection by appointment (phone number: 202–906–5922 or e-mail Public.Info@OTS.Treas.gov) at the Public Reading Room, 1700 G Street, NW., Washington, DC 20552, and the OTS Northeast Regional Office, Harborside Financial Center Plaza Five, Suite 1600, Jersey City, New Jersey 07311.

Dated: November 24, 2010.
By the Office of Thrift Supervision.
Sandra E. Evans,
Federal Register Liaison.