12 CFR 707.9 Enforcement and record retention.
(a) Administrative enforcement. Section 270 of TISA (12 U.S.C. 4309) contains the provisions relating to administrative sanctions for failure to comply with the requirements of TISA and this part.
(b) Civil liability. Section 271 of TISA (12 U.S.C. 4310) contains the provisions relating to civil liability for failure to comply with the requirements of TISA and this part; Section 271 is repealed effective September 30, 2001.
(c) Record retention. A credit union shall retain evidence of compliance with this regulation for a minimum of two years after the date disclosures are required to be made or action is required to be taken.

12 CFR 710.7 Retention of records.
(a) The board of directors or liquidating agent shall appoint a custodian for the Federal credit union's records which are to be retained after the final distribution of assets.
(b) All records of the liquidated Federal credit union necessary to establish that creditors were paid and that assets were equitably distributed to the members shall be retained by the custodian for a period of five years following the date of charter cancellation.

12 CFR 724.1 Federal Credit Unions acting as trustees and custodians of certain tax-advantaged savings plans.
A federal credit union is authorized to act as trustee or custodian, and may receive reasonable compensation for so acting, under any written trust instrument or custodial agreement created or organized in the United States and forming part of a tax-advantaged savings plan which qualifies or qualified for specific tax treatment under sections 223, 401(d), 408, 408A and 530 of the Internal Revenue Code (26 U.S.C. 223, 401(d), 408, 408A and 530), for its members or groups of its members, provided the funds of such plans are invested in share accounts or share certificate accounts of the Federal credit union. Federal credit unions located in a territory, including the trust territories, or a possession of the United States, or the Commonwealth of Puerto Rico, are also authorized to act as trustee or custodian for such plans, if authorized under sections 223, 401(d), 408, 408A and 530 of the Internal Revenue Code as applied to the territory or possession under similar provisions of territorial law. All funds held in a trustee or custodial capacity must be maintained in accordance with applicable laws and rules and regulations as may be promulgated by the Secretary of Labor, the Secretary of the Treasury, or any other authority exercising jurisdiction over such trust or custodial accounts. The federal credit union shall maintain individual records for each participant which show in detail all transactions relating to the funds of each participant or beneficiary.

12 CFR 748.1 Filing of reports.
(a) Compliance report. Each federally insured credit union shall file with the regional director an annual statement certifying its compliance with the requirements of this part. The statement shall be dated and signed by the president or other managing officer of the credit union. The statement is contained on the Report of Officials which is submitted annually by federally insured credit unions after the election of officials. In the case of federally insured state-chartered credit unions, this statement can be mailed to the regional director via the state supervisory authority, if desired. In any event, a copy of the statement shall always be sent to the appropriate state supervisory authority.
(b) Catastrophic act report. Each federally insured credit union will notify the regional director within 5 business days of any catastrophic act that occurs at its office(s). A catastrophic act is any disaster, natural or otherwise, resulting in physical destruction or damage to the credit union or causing an interruption in vital member services, as defined in §749.1 of this chapter, projected to last more than two consecutive business days. Within a reasonable time after a catastrophic act occurs, the credit union shall ensure that a record of the incident is prepared and filed at its main office. In the preparation of such record, the credit
union should include information sufficient to indicate the office where the catastrophic act occurred; when it took place; the amount of the loss, if any; whether any operational or mechanical deficiency(ies) might have contributed to the catastrophic act; and what has been done or is planned to be done to correct the deficiency(ies).

(c) Suspicious Activity Report. A credit union must file a report if it knows, suspects, or has reason to suspect that any crime or any suspicious transaction related to money laundering activity or a violation of the Bank Secrecy Act has occurred. For the purposes of this paragraph (c) credit union means a federally-insured credit union and official means any member of the board of directors or a volunteer committee.

(1) Reportable activity. Transaction for purposes of this paragraph means a deposit, withdrawal, transfer between accounts, exchange of currency, loan, extension of credit, purchase or sale of any stock, bond, share certificate, or other monetary instrument or investment security, or any other payment, transfer, or delivery by, through, or to a financial institution, by whatever means effected. A credit union must report any known or suspected crime or any suspicious transaction related to money laundering or other illegal activity, for example, terrorism financing, loan fraud, or embezzlement, or a violation of the Bank Secrecy Act by sending a completed suspicious activity report (SAR) to the Financial Crimes Enforcement Network (FinCEN) in the following circumstances:

(i) Insider abuse involving any amount. Whenever the credit union detects any known or suspected Federal crime, or pattern of criminal violations, committed or attempted against the credit union or involving a transaction or transactions conducted through the credit union, where the credit union believes it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the credit union was used to facilitate a criminal transaction, and the credit union has a substantial basis for identifying one of the credit union's officials, employees, or agents as having committed or aided in the commission of the criminal violation, regardless of the amount involved in the violation;

(ii) Transactions aggregating $5,000 or more where a suspect can be identified. Whenever the credit union detects any known or suspected Federal crime, or pattern of criminal violations, committed or attempted against the credit union or involving a transaction or transactions conducted through the credit union, and involving or aggregating $5,000 or more in funds or other assets, where the credit union believes it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the credit union was used to facilitate a criminal transaction, and the credit union has a substantial basis for identifying a possible suspect or group of suspects. If it is determined before filing this report that the identified suspect or group of suspects has used an alias, then information regarding the true identity of the suspect or group of suspects, as well as alias identifiers, such as drivers' licenses or social security numbers, addresses and telephone numbers, must be reported;

(iii) Transactions aggregating $25,000 or more regardless of potential suspects. Whenever the credit union detects any known or suspected Federal crime, or pattern of criminal violations, committed or attempted against the credit union or involving a transaction or transactions conducted through the credit union, involving or aggregating $25,000 or more in funds or other assets, where the credit union believes it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the credit union was used to facilitate a criminal transaction, even though the credit union has no substantial basis for identifying a possible suspect or group of suspects; or

(iv) Transactions aggregating $5,000 or more that involve potential money laundering or violations of the Bank Secrecy Act. Any transaction conducted or attempted by, at or through the credit union and involving or aggregating $5,000 or more in funds or other assets, if the credit union knows, suspects, or has reason to suspect:

(A) The transaction involves funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any Federal law or regulation or to avoid any transaction reporting requirement under Federal law;

(B) The transaction is designed to evade any regulations promulgated under the Bank Secrecy Act; or

(C) The transaction has no business or apparent lawful purpose or is not the sort of transaction in which the particular member would normally be expected to engage, and the credit union knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.
(v) Exceptions. A credit union is not required to file a SAR for a robbery or burglary committed or attempted that is reported to appropriate law enforcement authorities, or for lost, missing, counterfeit, or stolen securities and the credit union files a report pursuant to the reporting requirements of 17 CFR 240.17f–1.

(2) Filing Procedures. (i) Timing. A credit union must file a SAR with FinCEN no later than 30 calendar days from the date the suspicious activity is initially detected, unless there is no identified suspect on the date of detection. If no suspect is identified on the date of detection, a credit union may use an additional 30 calendar days to identify a suspect before filing a SAR. In no case may a credit union take more than 60 days from the date it initially detects a reportable transaction to file a SAR. In situations involving violations requiring immediate attention, such as ongoing money laundering schemes, a credit union must immediately notify, by telephone, an appropriate law enforcement authority and its supervisory authority, in addition to filing a SAR.

(ii) Content. A credit union must complete, fully and accurately, SAR form TDF 90–22.47, Suspicious Activity Report (also known as NCUA Form 2362) in accordance with the form’s instructions and 31 CFR Part 103.18. A copy of the SAR form may be obtained from the credit union resources section of NCUA’s Web site, http://www.ncua.gov, or the regulatory section of FinCEN’s Web site, http://www.fincen.gov. These sites include other useful guidance on SARs, for example, forms and filing instructions, Frequently Asked Questions, and the FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual.

(iii) Compliance. Failure to file a SAR as required by the form’s instructions and 31 CFR Part 103.18 may subject the credit union, its officials, employees, and agents to the assessment of civil money penalties or other administrative actions.

(3) Retention of Records. A credit union must maintain a copy of any SAR that it files and the original or business record equivalent of all supporting documentation to the report for a period of five years from the date of the report. Supporting documentation must be identified and maintained by the credit union as such. Supporting documentation is considered a part of the filed report even though it should not be actually filed with the submitted report. A credit union must make all supporting documentation available to appropriate law enforcement authorities and its regulatory supervisory authority upon request.

(4) Notification to board of directors. (i) Generally. The management of the credit union must promptly notify its board of directors, or a committee designated by the board of directors to receive such notice, of any SAR filed.

(ii) Suspect is a director or committee member. If a credit union files a SAR and the suspect is a director or member of a committee designated by the board of directors to receive notice of SAR filings, the credit union may not notify the suspect, pursuant to 31 U.S.C. 5318(g)(2), but must notify the remaining directors, or designated committee members, who are not suspects.

(5) Confidentiality of reports. SARs are confidential. Any credit union, including its officials, employees, and agents, subpoenaed or otherwise requested to disclose a SAR or the information in a SAR must decline to produce the SAR or to provide any information that would disclose that a SAR was prepared or filed, citing this part, applicable law, for example, 31 U.S.C. 5318(g), or both, and notify NCUA of the request. A credit union must make the filed report and all supporting documentation available to appropriate law enforcement authorities and its regulatory supervisory authority upon request.

(6) Safe Harbor. Any credit union, including its officials, employees, and agents, that makes a report of suspected or known criminal violations and suspicious activities to law enforcement and financial institution supervisory authorities, including supporting documentation, are protected from liability for any disclosure in the report, or for failure to disclose the existence of the report, or both, to the full extent provided by 31 U.S.C. 5318(g)(3). This protection applies if the report is filed pursuant to this part or is filed on a voluntary basis.

12 CFR 748.2 Procedures for monitoring Bank Secrecy Act (BSA) compliance.

(a) Purpose. This section is issued to ensure that all federally-insured credit unions establish and maintain procedures reasonably designed to assure and monitor compliance with the requirements of subchapter II of chapter 53 of title 31, United States Code, the Financial Recordkeeping and Reporting of Currency and Foreign Transactions Act, and the implementing regulations promulgated thereunder by the Department of Treasury, 31 CFR part 103.
(b) Establishment of a BSA compliance program — (1) Program requirement. Each federally-insured credit union shall develop and provide for the continued administration of a program reasonably designed to assure and monitor compliance with the recordkeeping and recording requirements set forth in subchapter II of chapter 53 of title 31, United States Code and the implementing regulations issued by the Department of the Treasury at 31 CFR part 103. The compliance program must be written, approved by the credit union's board of directors, and reflected in the minutes of the credit union.

(2) Customer identification program. Each federally-insured credit union is subject to the requirements of 31 U.S.C. 5318(l) and the implementing regulation jointly promulgated by the NCUA and the Department of the Treasury at 31 CFR 103.121, which require a customer identification program to be implemented as part of the BSA compliance program required under this section.

(c) Contents of compliance program. Such compliance program shall at a minimum—

(1) Provide for a system of internal controls to assure ongoing compliance;

(2) Provide for independent testing for compliance to be conducted by credit union personnel or outside parties;

(3) Designate an individual responsible for coordinating and monitoring day-to-day compliance; and

(4) Provide training for appropriate personnel.

12 CFR 749.2 Vital records preservation program.
The board of directors of a credit union is responsible for establishing a vital records preservation program within 6 months after its insurance certificate is issued. The program must be in writing and contain procedures for maintaining duplicate vital records at a vital records center. The procedures must include: designated staff responsible for vital records preservation, a schedule for the storage and destruction of records, and a records preservation log detailing for each record stored, its name, storage location, storage date, and name of the person sending the record for storage. It is recommended credit unions include in these procedures a method for using duplicate records to restore vital member services in the event of catastrophic act. Credit unions which have some or all of their records maintained by an off-site data processor are considered to be in compliance for the storage of those records if the service agreement specifies the data processor safeguards against the simultaneous destruction of production and back-up information.

12 CFR 749.3 Vital records center.
A vital records center is defined as a storage facility, which may include another federally-insured credit union, at any location far enough from the credit union's offices to avoid the simultaneous loss of both sets of records in the event of a catastrophic act. A credit union must maintain or contract with a third party to maintain any equipment or software for its vital records center necessary to access records.

12 CFR 749 Record Retention Guidelines
Credit unions often look to NCUA for guidance on the appropriate length of time to retain various types of operational records. NCUA does not regulate in this area, but as an aid to credit unions it is publishing this appendix of suggested guidelines for record retention. NCUA recognizes that credit unions must strike a balance between the competing demands of space, resource allocation and the desire to retain all the records that they may need to conduct their business successfully. Efficiency requires that all records that are no longer useful be discarded, just as both efficiency and safety require that useful records be preserved and kept readily available.

A. What Format Should the Credit Union Use for Retaining Records?
NCUA does not recommend a particular format for record retention. If the credit union stores records on microfilm, microfiche, or in an electronic format, the stored records must be accurate, reproducible and accessible to an NCUA examiner. If records are stored on the credit union premises, they should be immediately accessible upon the examiner's request; if records are stored by a third party or off-site, then they should be made available to the examiner within a reasonable time after the examiner's request. The credit union must maintain the necessary equipment or software to permit an examiner to review and
reproduce stored records upon request. The credit union should also ensure that the reproduction is acceptable for submission as evidence in a legal proceeding.

B. Who Is Responsible for Establishing a System for Record Disposal?
The credit union’s board of directors may approve a schedule authorizing the disposal of certain records on a continuing basis upon expiration of specified retention periods. A schedule provides a system for disposal of records and eliminates the need for board approval each time the credit union wants to dispose of the same types of records created at different times.

C. What Procedures Should a Credit Union Follow When Destroying Records?
The credit union should prepare an index of any records destroyed and retain the index permanently. Destruction of records should ordinarily be carried out by at least two persons whose signatures, attesting to the fact that records were actually destroyed, should be affixed to the listing.

D. What Are the Recommended Minimum Retention Times?
Record destruction may impact the credit union’s legal standing to collect on loans or defend itself in court. Since each state can impose its own rules, it is prudent for a credit union to consider consulting with local counsel when setting minimum retention periods. A record pertaining to a member's account that is not considered a vital record may be destroyed once it is verified by the supervisory committee. Individual Share and Loan Ledgers should be retained permanently. Records, for a particular period, should not be destroyed until both a comprehensive annual audit by the supervisory committee and a supervisory examination by the NCUA have been made for that period.

E. What Records Should Be Retained Permanently?
1. Official records of the credit union that should be retained permanently are:
   (a) Charter, bylaws, and amendments.
   (b) Certificates or licenses to operate under programs of various government agencies, such as a certificate to act as issuing agent for the sale of U.S. savings bonds.
   (c) Current manuals, circular letters and other official instructions of a permanent character received from the NCUA and other governmental agencies.
2. Key operational records that should be retained permanently are:
   (a) Minutes of meetings of the membership, board of directors, credit committee, and supervisory committee.
   (b) One copy of each NCUA 5300 financial report or its equivalent.
   (c) One copy of each supervisory committee comprehensive annual audit report and attachments.
   (d) Supervisory committee records of account verification.
   (e) Applications for membership and joint share account agreements.
   (f) Journal and cash record.
   (g) General ledger.
   (h) Copies of the periodic statements of members, or the individual share and loan ledger. (A complete record of the account should be kept permanently.)
   (i) Bank reconciliations.
   (j) Listing of records destroyed.

F. What Records Should a Credit Union Designate for Periodic Destruction?
Any record not described above is appropriate for periodic destruction unless it must be retained to comply with the requirements of consumer protection regulations. Periodic destruction should be scheduled so that the most recent of the following records are available for the annual supervisory committee audit and the NCUA examination. Records that may be periodically destroyed include:
(a) Applications of paid off loans.
(b) Paid notes.
(c) Various consumer disclosure forms, unless retention is required by law.
(d) Cash received vouchers.
(e) Journal vouchers.
(f) Canceled checks.
(g) Bank statements.
(h) Outdated manuals, canceled instructions, and nonpayment correspondence from the NCUA and other governmental agencies.

12 CFR 791.17 Maintenance of meeting records.
(a) Except in those circumstances which are beyond the control of the agency, the Board shall maintain a complete transcript or electronic recording adequate to record fully the proceedings of each meeting, or any portion thereof, closed to public observation. However, for meetings closed under §791.12(a) (8), (9)(i) or (10), the Board shall maintain either a transcript, a recording or a set of minutes. The Board shall maintain a complete electronic recording for each open meeting or any portion thereof. All records shall clearly identify each speaker.
(b) A set of minutes shall fully and clearly describe all matters discussed and shall provide a full and accurate summary of any actions taken, and the reasons for taking such action. Minutes shall also include a description of each of the views expressed by each person in attendance on any item and the record of any roll call vote, reflecting the vote of each member. All documents considered in connection with any action shall be identified in the minutes.
(c) The agency shall maintain a complete verbatim copy of the transcript, a complete copy of the minutes or a complete electronic recording of each meeting, or any portion of a meeting, closed to public observation, for at least two years after such meeting or for one year after the conclusion of any agency proceeding with respect to which the meeting or any portion was held, whichever occurs later. The agency shall maintain a complete electronic recording of each open meeting for at least three months after the meeting date. A complete set of minutes shall be maintained on a permanent basis for all meetings.