(c) Each Federal credit union, as part of its information security program, must properly dispose of any consumer information the Federal credit union maintains or otherwise possesses, as required under § 717.83 of this chapter.

[50 FR 53295, Dec. 31, 1985, as amended at 53 FR 4845, Feb. 18, 1988; 66 FR 8161, Jan. 30, 2001; 69 FR 69274, Nov. 29, 2004; 70 FR 22778, May 2, 2005]

§ 748.1 Filing of reports.

(a) The president or managing official of each federally insured credit union must certify compliance with the requirements of this part in its Credit Union Profile annually through NCUA's online information management system.

(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) ***Cyber incident report.*** Each federally insured credit union must notify the appropriate NCUA-designated point of contact of the occurrence of a *reportable cyber incident* via email, telephone, or other similar methods that the NCUA may prescribe. The NCUA must receive this notification as soon as possible but no later than 72 hours after a federally insured credit union reasonably believes that it has experienced a reportable cyber incident or, if reporting pursuant to paragraph (c)(1)(i)(C) of this section, within 72 hours of being notified by a third-party, whichever is sooner.

(1) ***Reportable cyber incident.***

(i) A reportable cyber incident is any substantial cyber incident that leads to one or more of the following:

(A) A substantial loss of confidentiality, integrity, or availability of a network or member information system as defined in appendix A, section I.B.2. e., of this part that results from the unauthorized access to or exposure of sensitive data, disrupts vital member services as defined in § 749.1 of this chapter, or has a serious impact on the safety and resiliency of operational systems and processes.

(B) A disruption of business operations, vital member services, or a member information system resulting from a cyberattack or exploitation of vulnerabilities.

(C) A disruption of business operations or unauthorized access to sensitive data facilitated through, or caused by, a compromise of a credit union service organization, cloud service provider, or other third-party data hosting provider or by a supply chain compromise.

(ii) A *reportable cyber incident* does not include any event where the cyber incident is performed in good faith by an entity in response to a specific request by the owner or operators of the system.

(2) ***Definitions.*** For purposes of this part:

Compromise means the unauthorized disclosure, modification, substitution, or use of sensitive data or the unauthorized modification of a security-related system, device, or process in order to gain unauthorized access.

Confidentiality means preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Cyber incident means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system.

Cyberattack means an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

Disruption means an unplanned event that causes an information system to be inoperable for a length of time.

Integrity means guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.

Sensitive data means any information which by itself, or in combination with other information, could be used to cause harm to a credit union or credit union member and any information concerning a person or their account which is not public information, including any non-public personally identifiable information.

(d) ***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 criminal violations, 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 criminal violation, 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 criminal violation, 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 1020.320. 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 1020.320 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.

[50 FR 53295, Dec. 31, 1985, as amended at 53 FR 26232, July 12, 1988; 58 FR 17492, Apr. 5, 1993; 61 FR 11527, Mar. 21, 1996; 71 FR 62878, Oct. 27, 2006; 72 FR 42273, Aug. 2, 2007; 74 FR 35769, July 21, 2009; 76 FR 18366, Apr. 4, 2011; 78 FR 64885, Oct. 30, 2013; 88 FR 12816, Mar. 1, 2023]