**1663:
NCUA Guidance – SAR Reporting in a Cyber Incident**

**Model Content Published Date: 11/26/2024**

**Suspicious Activity Report - Cyber Incident**

The credit union will file a Suspicious Activity Report (“SAR”), if required by applicable federal regulations. In situations involving federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing, the credit union will immediately notify, by telephone, appropriate law enforcement authorities and NCUA or its primary state regulator, in addition to filing a timely SAR.

From FINCEN (United States Department of the Treasury Financial Crimes Enforcement Network) advisory letter FIN-2016-A0052: <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a005>

*A financial institution is required to report a suspicious transaction conducted or attempted by, at, or through the institution that involves or aggregates to $5,000 or more in funds or other assets. If a financial institution knows, suspects, or has reason to suspect that a cyber-event was intended, in whole or in part, to conduct, facilitate, or affect a transaction or a series of transactions, it should be considered part of an attempt to conduct a suspicious transaction or series of transactions. Cyber-events targeting financial institutions that could affect a transaction or series of transactions would be reportable as suspicious transactions because they are unauthorized, relevant to a possible violation of law or regulation, and regularly involve efforts to acquire funds through illegal activities.*

*When filing a mandatory or voluntary SAR involving a cyber-event, financial institutions should provide complete and accurate information, including relevant facts in appropriate SAR fields, and information about the cyber-event in the narrative section of the SAR—in addition to any other related suspicious activity.*

To the extent available, ***SARs involving cyber-events should include***:

* Description and magnitude of the event
* Known or suspected time, location, and characteristics or signatures of the event
* Indicators of compromise
* Relevant IP addresses and their timestamps
* Device identifiers
* Methodologies used
* Other information the institution believes is relevant