Northwest Credit Union Association
Idaho • Oregon • Washington

Regulatory Update: NCUA Actions
April 16, 2020

At its April 16, 2020, meeting, the NCUA board took many important actions, including:

- Adoption of the interagency appraisal rule that other regulatory agencies adopted earlier this week;
- Finalization of the appraisal rule, which increases the threshold on consumer mortgages requiring no appraisal to $400,000; and
- Approval of changes to occupancy and participation requirements through an interim final rule.

The NCUA also has sent two recent letters of interest to credit unions, one outlining changes to the Central Liquidity Fund, and the other sharing cybersecurity expectations for credit union staff working from home.

Regulatory Changes to the Central Liquidity Fund

The NCUA Board approved an interim final rule to make additional enhancements to the NCUA's CLF rule, Part 725. In addition to the legislative changes described in this letter, these enhancements add more flexibility and relief for credit unions. It will be easier to join the CLF and access liquidity if the need arises as a regular member or through your corporate credit union as part of an agent relationship. The NCUA's regulatory changes include the following permanent and temporary relief measures:

- Permanently eliminate the six-month waiting period for a new member to receive a loan. The prior § 725.3 provided that, with limited exception, any credit union that became a regular member of the CLF could not receive a CLF loan without approval of the NCUA Board for six months after becoming a member. Under the new rule, new regular and agent members can borrow as soon as they complete the new member documents and pay the required capital stock amount. The NCUA Board believes this is a necessary change to ensure the availability of liquidity assistance to all eligible CLF members at the earliest opportunity.
- Temporarily amend the waiting period for a credit union to terminate its CLF membership. Previously, a CLF member could terminate its membership only after 6 to 24 months, based on the size of the credit union's stock subscription in the CLF. This requirement has been temporarily amended by the NCUA Board to encourage eligible credit unions to join the CLF now. A credit union that requests withdrawal of its CLF membership in writing to the NCUA Board between publication of the interim final rule and Dec. 31, 2020, will wait no longer than 6 months for that withdrawal to take effect. Any credit union that retains CLF membership after Dec. 31, 2020, may immediately terminate its membership before Dec. 31, 2021, after providing written notice to the NCUA Board. After Dec. 31, 2021, the temporary termination provisions will expire and a credit union could terminate its membership after 6 or 24 months, based on the size of its stock subscription in the CLF. This provision applies to existing members and credit unions that become members before Dec. 31, 2020.

A temporary CLF membership during the COVID-19 pandemic will greatly benefit the credit union system. The more capital subscriptions the CLF has, the higher the borrowing authority the CLF and the NCUA have, to provide liquidity assistance to credit unions.

- Permanently ease collateral requirements. The prior § 725.19 required each CLF loan and each agent loan to be secured by a first-priority security interest in collateral of the credit union with a net book value at least equal to 110% of all amounts due under the applicable loan, or by guarantee of the Share Insurance Fund. Under the new rule, the amount of collateral will be determined from the CLF's collateral margins table, published on the NCUA's website. The required collateral percentages vary based on different types of assets, and in some cases, *less* than 110% will be required. This change eases the collateral requirements, allowing a greater amount of borrowing overall.

- Temporarily permit an agent member to borrow for its own liquidity needs. Previously, the CLF could only meet the liquidity needs of natural-person credit unions. The interim final rule includes several provisions that align with the CARES Act change that allows an agent member to borrow from the CLF for its own liquidity needs. Specifically, the amendments clarify that an agent member may borrow from the CLF for its own liquidity needs after subscribing to the capital stock of the CLF in an amount equal to one-half of one percent of the agent's own paid-in and unimpaired capital and surplus. Expanding the liquidity resources of corporate credit unions, even temporarily, is an added measure of liquidity strength for the system as a whole. A loan to an Agent for its own needs would be subject to the same creditworthiness and liquidity-need criteria as for all other member loans.

Credit Unions are Encouraged to Join the CLF as Soon as Possible

CLF membership provides both individual and systemic benefits by serving as a form of liquidity insurance for individual credit unions (including corporate credit unions temporarily) and the broader credit union system. CLF members may borrow for their own liquidity needs and earn a quarterly dividend on their capital stock. CLF stock subscriptions provide the credit union system and the Share Insurance Fund a vital contingent source of funds to assist with system-wide liquidity events, which may be necessary in addressing the impact of the COVID-19 pandemic on individual credit unions, groups of credit unions, and the Share Insurance Fund.

Membership in the CLF is affordable and relatively easy. A credit union may become a CLF member by completing a membership application and contributing one-half of its stock subscription requirement, which equates to approximately one-fourth of one-percent (0.0025 percent) of a credit union's assets. Visit the CLF webpage for more information on becoming a member.

The NCUA has confidence that the credit union system will remain safe and sound. The reforms described in this letter are designed to allow credit unions and the NCUA to navigate this extraordinary and unprecedented time and to ensure the availability of enough liquidity until the extent of the COVID-19 impact on credit unions has been fully determined. If you have questions about the changes described in this letter or CLF membership, please contact the CLF at clfmail@ncua.gov.

Preparing Employees to Prevent Security Incidents

Common cybersecurity risks for remote workers include:

- Malware attacks;
- Phishing and other social engineering attacks; and
- Advance Persistent Threat (APT) attacks.

To minimize the risk of a cyberattack while credit union staff is working remotely or with personal equipment, policies and procedures should address employee requirements, such as:

- Ensuring that family members or others do not use devices designated for work;
- Implementing session time-outs and encryption of sensitive information;
- Keeping devices physically secure;
- Working with a user account and not an administrator or privileged account;
- Establishing strong, unique passwords for all logins and devices on their home network;
- Leveraging firewall capabilities available through internet service providers;
- Increasing wireless security to the strongest encryption option;
- Removing unnecessary services and software;
- Updating software regularly;
- Maintaining antivirus software and ensuring timely updates to definitions; and
- Ensuring system and account logs are being collected and maintained.

Credit union management should communicate proactively with employees to verify that remote work is being done securely and should provide guidance and assistance as needed. Additional institution-level controls, such as those designed to ensure operating system versions, patch levels, and anti-malware solutions meet your security standards, should be addressed in your risk assessment.

Responding to a Security Incident

To minimize the impact of an attack, policies and procedures should address the immediate actions an employee should take when they suspect a cyberattack, such as:

- Disconnecting the device(s) from all internet connectivity;
- Keeping the computer on to preserve forensic evidence; and
- Reporting the incident to their organization.

Policies and procedures should also address how the credit union would respond to a security incident, such as:

- Filing a report with local law enforcement or other law enforcement agencies, such as the FBI Internet Crime Complaint Center;
- Taking appropriate corrective action, depending on the nature of the incident (for example, changing passwords, completing a forensic audit, and scanning and cleaning devices); and
- Evaluating whether the incident should be reported to the NCUA or state supervisory authority.

Cybersecurity Resources

The following resources provide additional information on cybersecurity risks and working remotely:

- Department of Homeland Security Cybersecurity and Infrastructure Security Agency, Security Tips for Home Network Security;
- National Institute for Standards and Technology Special Publication 800-46r2, Guide to Enterprise Telework, Remote Access and Bring Your Own Device (BYOD) Security; and
- Information Sharing and Analysis Organization groups, such as the Financial Services Information Sharing and Analysis Center and the National Credit Union Information Sharing and Analysis Organization.

The Information Sharing and Analysis Organization has a complete list of Information Sharing Groups on its website.

While funds remain available, the NCUA's Office of Credit Union Resources and Expansion has several grants and loans available that may be of use to your institution. If you have questions about cybersecurity, please contact your regional office or state supervisory authority.

We are pleased to provide this regulatory update. Reach out to John Trull, VP, Regulatory Affairs for NWCUA, if we can be of assistance.