



**America's
Credit Unions**

Jim Nussle
President & CEO
202-508-6745
jnussle@americascreditunions.org

99 M Street SE
Suite 300
Washington, DC 20003

February 6, 2024

The Honorable Patrick McHenry
Chairman
Committee on Financial Services
U.S. House of Representatives
Washington, DC 20515

The Honorable Maxine Waters
Ranking Member
Committee on Financial Services
U.S. House of Representatives
Washington, DC 20515

Re: Today's Hearing: "The Annual Report of the Financial Stability Oversight Council"

Dear Chairman McHenry and Ranking Member Waters:

On behalf of America's Credit Unions, I am writing regarding the Committee's hearing with Treasury Secretary Janet Yellen entitled, "The Annual Report of the Financial Stability Oversight Council." America's Credit Unions is the voice of consumers' best option for financial services: credit unions. We advocate for policies that allow the industry to effectively meet the needs of their nearly 140 million members nationwide.

Third Party Vendor Authority for NCUA in FSOC Annual Report

America's Credit Unions and our member credit unions believe that cybersecurity, including the security of vendors that credit unions do business with, is an important issue that demands sector-wide coordination. However, we are opposed to granting additional authority to the National Credit Union Administration (NCUA) to examine third parties. We believe in a strong NCUA, but we also believe that the NCUA should stay focused on where its expertise lies: regulating credit unions.

There are other tools already in place for the NCUA to get access to information about credit union vendors. We believe the agency's time and resources are better focused on reducing regulatory burden by coordinating efforts among the financial regulators. The NCUA sits on the Federal Financial Institutions Examination Council (FFIEC) with the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency, and the Federal Reserve. The FFIEC was created to coordinate examination findings and approach in the name of consistency and to avoid duplication. This means that as a member of the FFIEC, the NCUA should be able to request the results of an examination of a core processor from the other regulators and not have to send another exam team from the NCUA into their business and duplicate an examination.

The NCUA is best positioned to act as an aggregator or amplifier of threat intelligence assembled by other private or government sources. Sharing relevant cybersecurity information with credit unions does not depend on gathering intelligence through a duplicative supervision program. An August 2023 report from the FDIC's Office of the Inspector General (OIG) states that "[a]ccording to FDIC officials, other U.S. government and private sector entities are proficient at providing threat information to financial institutions," and further notes that "[h]istorically,

the FDIC's Division of Risk Management Supervision (RMS) has shared relevant cyber threat and vulnerability information with financial institutions prepared by other sources, such as the DHS CISA, the Treasury Department, and the FBI." While the FDIC does possess internally compiled threat and vulnerability information relevant to the banks it supervises, the agency's Inspector General has recommended that "the FDIC share FDIC-developed threat and vulnerability information with financial institutions or other financial sector entities." Such information sharing, if extended to the NCUA, would offer a straightforward and effective pathway for enhancing the NCUA's early warning capabilities and protecting credit unions.

America's Credit Unions and our credit union members recognize the importance of mitigating vulnerabilities to the financial system. However, there are more efficient ways to proceed. Instead of granting the NCUA vendor examination authority, Congress should encourage the agency to use the FFIEC and gain access to the information on exam findings on companies that have already been examined by other regulators. If that option is not available for the NCUA due to the decisions of the other FFIEC regulators, Congress should consider compelling the other regulators to share such information with the NCUA. This would be a preferable route than raising costs on credit unions and their 140 million members for the creation of a duplicative NCUA program with uncertain scope. Supervisory reports for core providers will likely have significant cross-applicability; according to the NCUA, approximately five core processor vendors control approximately 85 percent of credit union data.

Furthermore, it is uncertain whether simply replicating the existing supervisory authorities of other federal banking regulators will reduce exploitation of third-party vulnerabilities. Recent trends suggest that a significant share of vulnerabilities lie dormant (*i.e.*, zero-day vulnerabilities) until they are exploited for the first time. Given the limited time and expertise available to probe the inner workings of proprietary vendor systems, a core component of service provider oversight is the sufficiency of risk and security controls documented in agreements between third parties and regulated institutions. The NCUA has codified these principles in its regulations. While federal financial regulators emphasize adoption of controls and appropriate governance over service providers, the role of detecting cybersecurity risks that exist outside of regulated institutions is more appropriately carried out by federal agencies with a cybersecurity or law enforcement mandate. The NCUA can benefit from this distributed expertise by focusing its attention on improving information sharing with Treasury and other FFIEC agencies.

Treasury can also support greater interagency collaboration through its role as the financial sector risk management agency supporting critical infrastructure activities. The most recently adopted Financial Services Sector-Specific Plan encourages Treasury to coordinate with law enforcement, the Department of Homeland Security (DHS), and financial regulators to share information about current and emerging threats.

Use of existing reports for other technology service providers would also address the NCUA's concerns without creating additional costs to credit unions or increasing regulatory burdens on credit unions and small businesses.

Cybersecurity

Treasury should ensure that future implementation of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCA) is consistent with existing mechanisms for reporting cyber incidents adopted by the NCUA and other federal banking agencies, to the extent certain financial institutions are regarded as critical infrastructure operators. Enacted in March 2022, the CIRCA assigns to the Cybersecurity and Infrastructure Security Agency (CISA) the responsibility for implementing by 2025 a cyber reporting framework for critical infrastructure owners (covered entities). The statutory parameters for this framework are already mirrored in current NCUA regulation.

Under the CIRCA, an exception to filing a cyber incident or ransomware report directly with CISA is available when CISA has an existing agreement in place with a covered entity's federal regulator and the covered entity is required by law, regulation, or contract to report substantially similar information to its federal regulator within a substantially similar timeframe. As the sector-specific agency coordinating critical infrastructure activities, Treasury should ensure that CISA is properly informed of the NCUA's existing reporting requirement. To ensure that credit unions can fully benefit from the CIRCA's provisions aimed at easing regulatory burden and avoiding duplication, we encourage Treasury to take all necessary steps to ensure that credit unions will only need to meet a single reporting standard administered by the NCUA.

CDFI Certification

America's Credit Unions greatly appreciates the work the Community Development Financial Institution (CDFI) Fund has done over the past few years to solicit and incorporate feedback as it updated its CDFI Certification Application and Agreement. Now that the application is released, many credit unions who have been waiting to become certified are beginning the process of evaluating their ability to qualify. Credit unions, banks, and loan funds that are certified as CDFIs are already working with their partners to assess their ability to recertify. While the Fund provided flexibility, clarity, and many changes to ensure that organizations that should be able to certify can, not all issues have been addressed.

First, the CDFI Fund's Target Market Assessment Methodologies require the collection of actual race and ethnicity data using Home Mortgage Disclosure Act procedures for CDFIs with certain target markets. Credit unions have raised significant concerns regarding the legality of this requirement and asked for governmental support to lend credibility in requesting that information, such as model form or signage to clarify the reason for the request. Treasury has indicated that it would coordinate with the other financial regulators to provide clarity regarding the legal and compliance risk related to the information collection. Treasury has also indicated it would consider providing additional support for this data collection. However, the CDFI Fund has finalized the requirement to obtain the data without providing any clarity or support. When asked, the Fund indicates it has not yet determined the best path to provide those answers. This is deeply concerning to affected credit unions.

Secondly, the CDFI Fund has not yet released the CDFI Certification Agreement which all CDFIs must execute in order to obtain certification. This agreement absolutely must be read in order

for organizations interested in certifying or recertifying to have a full understanding of the obligations associated with certification and the process that will happen should they fall out of compliance. The CDFI Certification Agreement was published for comment along with the CDFI Certification Application, but the Fund did not release the final version of the Certification Agreement with the Certification Application and to-date it has not indicated when it will be available.

Finally, many credit unions already report delays of multiple weeks in receiving responses from the CDFI Fund. It is predictable and understandable that the Fund has likely been inundated with applications for new certification and grant applications as the window for both of these is currently open. Further, the Fund is likely experiencing a flood of questions in response to the new application for recertifying CDFIs who cannot yet apply for recertification. However, the Fund has required that all 1,400+ existing CDFIs must apply for recertification in a 5-month window between August 1 and December 20 of this year. CDFIs that have not applied by December 20 will lose their certification. Given this compressed window, the number of CDFIs that must recertify, and the number of questions that will undoubtedly arise as CDFIs navigate a new application with each individual applicant's unique circumstances, it seems very likely that the volume of inquiries will exponentially grow as the year progresses. Against this backdrop, existing delays of 3-4 weeks for response is a deeply concerning indicator of the Fund's capacity to manage the coming workload. The CDFI Fund must be properly resourced to meet the needs of certifying and recertifying institutions and grant applications. America's Credit Unions urges Congress to identify where the operational shortfalls are at the Fund and to ensure that it has the appropriate funding to meet its mission and provide sufficient assistance to current and potential CDFI credit unions.

We also want to take this opportunity to express our strong support for H.R. 3161, the CDFI Fund Transparency Act, which would require annual testimony before the Committee from the Fund. We believe that this legislation is an important step to ensuring the successful operation of the Fund with these new changes.

Climate Risk

FSOC's Report on Climate-Related Financial Risk (Climate Report) included 35 recommendations to financial regulators on how to identify and address climate-related risks to the financial system. Last year, a status update on staff-level activities to support the Climate Report recommendations noted that all council member agencies have been building the capacity to address and understand climate-related risk. The FSOC status update cited a research note published by the NCUA regarding credit union exposure to climate-related physical risks, but offered no commentary regarding the soundness of the NCUA's methodology, or how the research compared to approaches taken by other financial regulators attempting to measure the financial impact of climate-related risk. The NCUA's research relies significantly on Federal Emergency Management Agency's (FEMA) National Risk Index (NRI) data to inform its assessments, and looked primarily at where a credit union's headquarters were located to assign a risk rating from the NRI at the county level, and then applied this rating to the credit union's entire balance sheet. We are concerned that this approach does not reflect a broader consensus

among financial regulators regarding the best method for assessing the financial impact of *physical* climate risks. More importantly, lack of methodological consensus could lead to an overestimation of projected risk for credit unions.

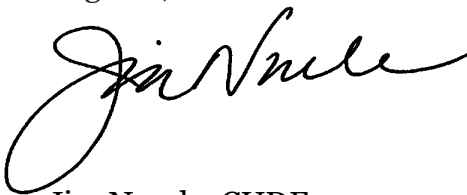
The NCUA also issued a request for information last year regarding how it might develop tools or procedures for assessing climate related risk. Any regulations or guidance issued to credit unions regarding climate-related financial risk should align with those of other federal banking regulators, and we encourage Treasury to facilitate such alignment through its role on the Climate-related Financial Risk Committee. If the NCUA were to impose more restrictive guidance or regulations on credit unions compared to other banking institutions, it could create a significant disadvantage for credit unions in terms of their viability and competitiveness. While we agree that climate risk is an area of risk for the agency to monitor, we wholeheartedly oppose any subsequent regulatory activity that would establish mandatory reporting procedures for credit unions or to otherwise prevent credit unions—directly or indirectly—from continuing to make independent business decisions as they deem most appropriate in order to serve their members.

Financial Institutions and the Greenhouse Gas Reduction Fund

The Inflation Reduction Act created the Greenhouse Gas Reduction Fund (GGRF) to provide funding for efforts to improve environmental impacts. Credit unions and CDFIs are well-positioned to use this program to help a number of American communities, including underserved and rural communities. Using regulated financial institutions that have experience in lending to local communities, and strong community ties, would seem to be the best way to implement the program. At a recent Energy and Commerce Subcommittee on Oversight and Investigations hearing, the Environmental Protection Agency (EPA) stated that it is working with several departments, including Treasury, in the evaluation and selection process. We encourage Treasury to advocate for financial institutions with the EPA as well and urge you to call on Secretary Yellen to do so.

On behalf of America's Credit Unions and the 140 million credit union members, thank you for holding this important hearing and considering our views on the subject.

Regards,



Jim Nussle, CUDE
President & CEO

cc: Members of the Committee on Financial Services