Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

May 10, 2024

Technology Service Providers and Credit Unions

This In Focus summarizes issues regarding the cybersecurity risks posed by third-party vendors that provide credit unions with technology services. It begins with background on the reliance on technology service providers (TSPs) by depositories (i.e., credit unions and commercial banks) and the ongoing concerns of their primary federal regulators. Next, the regulatory authorities that the National Credit Union Administration (NCUA), the primary federal regulator of credit unions, has over TSPs are compared to those of the three federal bank regulators—the Federal Reserve, the Office of the Comptroller of the Currency, and the Federal Deposit Insurance Corporation (FDIC). Specifically, the bank regulators have the authority to supervise TSPs used by banks, but the NCUA does not have the authority to supervise TSPs used by credit unions. The NCUA has requested that Congress grant it authority similar to the banking regulators' authority. A discussion of additional technology adoption challenges with implications for the credit union system follows.

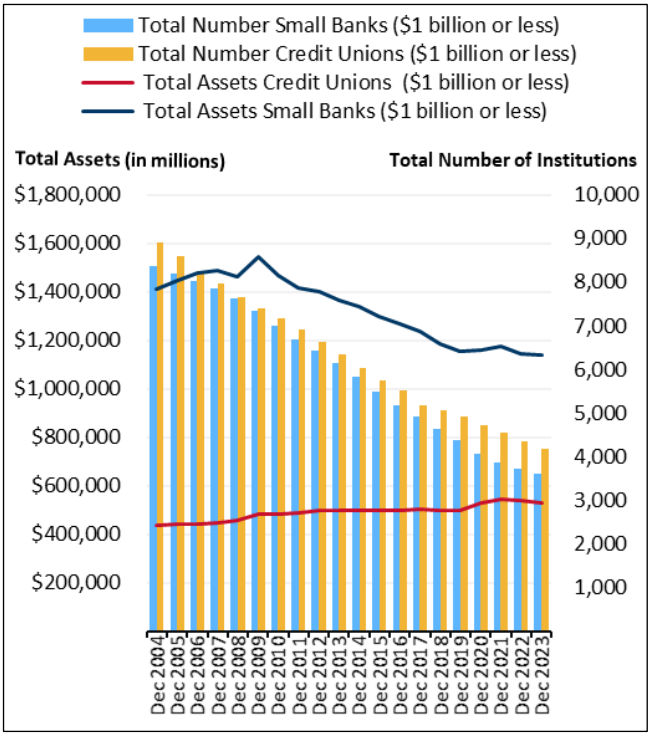
Background

As more financial transactions are conducted online, financial institutions that lack in-house technological expertise increasingly rely on third-party TSP vendors. TSPs develop software and interfaces for customer accounts and payment services, as well as cloud computing services for data storage. A survey of financial institutions released in 2023 shows a 91% increase in the adoption of cloud services since 2020. Credit unions have participated in this trend. With growing reliance on TSPs, the NCUA (as well as the federal bank regulators) is increasingly concerned with *operational risks*—the risk of loss having to do with failed internal controls, people, systems, or external events. Operational risks in the form of cyber-related disruptions (e.g., unauthorized access to customer data) can occur at either a depository or a TSP and may weaken public trust and confidence in the financial system. Operational risks can also increase the potential of *systemic risk*—widespread panic runs on depositories, especially under circumstances when multiple depositories rely on the same TSP that experiences a breach. On November 26, 2023, for example, the NCUA announced that a credit union TSP experienced a ransomware attack on its cloud services, affecting reportedly 60 credit unions and approximately 100,000 credit union members.

According to the U.S. Treasury's Office of Financial Research, the percentage of businesses affected by ransomware attacks rose from 79% to 87% in 2023. Furthermore, small depositories, which have limited resources for data security and rely more on TSPs, face heightened vulnerability compared to larger depositories. The NCUA cited a report noting that small depositories with less than $35 million in annual revenue are extremely vulnerable to hacking and malware breaches relative to their larger counterparts. Hence, many credit unions, which are generally smaller relative to many small banks, are arguably more vulnerable. **Figure 1** illustrates number and asset size differences between small credit unions and small banks, defining *small* as $1 billion or less in assets. Although small credit unions outnumber small banks, they collectively hold significantly fewer assets relative to the small banks. (For more information on similarities and differences between credit unions and banks, see CRS In Focus IF11048, *Introduction to Bank Regulation: Credit Unions and Community Banks: A Comparison*, by Darryl E. Getter.)

Figure 1. Small Credit Unions and Small Banks: Number of Firms and Total Assets

2004-2023



Source: CRS using data provided by the FDIC and NCUA.

Regulatory Authority Over TSPs

Bank regulators have a broad set of authorities to supervise vendors, such as TSPs, that have contractual relationships with banks. The Bank Service Company Act (P.L. 87-856) provides bank regulators with the authority to examine and regulate TSPs that provide services to banks, including check and deposit sorting as well as posting, preparation of statements, notices, bookkeeping, and accounting. Therefore, using vendors does not reduce a bank's responsibility to ensure that the actions of contractors are performed in a safe and sound manner. Activities conducted

through a TSP must meet the same regulatory requirements as if they were performed by the bank itself. For example, bank regulators may conduct formal on-site examinations of bank TSP cloud providers, as the Federal Reserve did in April 2019.

By contrast, NCUA lacks the same authorities held by the banking regulators. In a March 2022 report, the NCUA discussed not having examination, enforcement, or corrective action authority over TSPs, including credit union service organizations (CUSOs) that are wholly or partly owned by credit unions and provide financial support services for credit unions and their members. The report notes that the Examination Parity and Year 2000 Readiness for Financial Institutions Act (P.L. 105-164) gave the NCUA temporary authority over TSPs and CUSOs as part of Y2K readiness, which expired on December 31, 2001. On October 27, 2021, the NCUA expanded the list of permissible activities and services that CUSOs can perform, thus increasing the need for greater vendor authorities.

Section 501 of the Gramm-Leach-Bliley Act (P.L. 106-102) requires financial institutions to ensure the security and confidentiality of customer information. Therefore, despite its lack of authority over TSPs, the NCUA uses its supervisory authority over credit unions to help mitigate cybersecurity risks through requirements and guidance. For example, NCUA has adopted a cyber incident notification framework, which includes requirements for credit unions to follow when a cyber incident occurs. In addition, NCUA provides credit unions with guidance on how to evaluate third-party TSP relationships. NCUA also provides updated information about ransomware threats and attacks.

Despite these efforts, the NCUA still seeks the restoration of previous authority that would be similar to that of the banking regulators over TSPs. Without this authority, the NCUA notes that operational risks increase—not only for credit unions but also for the National Credit Union Share Insurance Fund, which is the federal deposit insurance fund for credit unions. The ability to supervise TSPs would potentially reduce possible losses to the fund that would be borne by the credit union system and taxpayers. The Financial Stability Oversight Council also recommends that Congress pass legislation providing adequate examination and enforcement powers to the NCUA, along with other relevant agencies (e.g., the Federal Housing Financing Agency), to oversee TSPs that interact with regulated entities.

Credit union trade groups, however, have opposed restoring NCUA's authority over credit union TSPs. The opposition arises due to an anticipated increase in costs for the NCUA to hire specialized examiners, which would be covered by levying additional fees on credit unions unless the legislation provided another funding source. The trade groups recommend that the NCUA use its existing authority to obtain information from CUSOs, which are already owned by credit unions. In addition, they argue that the NCUA—as a member of the Federal Financial Institutions Examination Council, an interagency body of federal financial regulators including the banking regulators—should be able to gain access to TSP examinations conducted by other council member agencies when a TSP serves both credit unions and banks. If the NCUA is not granted access, they argue that Congress should compel the other regulators to provide them with access.

Legislation has been introduced to address these issues. In the 117th Congress, S. 4698, the Improving Cybersecurity of Credit Unions Act, was introduced and referred to the Senate Banking, Housing, and Urban Affairs Committee. In the 118th Congress, H.R. 7036, the Strengthening Cybersecurity for the Financial Sector Act of 2024, was introduced on January 18, 2024. These bills would give NCUA the authority to regulate TSPs, among other things.

Additional Technology Challenges

Small financial institutions—particularly those providing financial services primarily to underserved communities, which would include mission-driven credit unions—face significant challenges when attempting to acquire new technologies. The Government Accountability Office notes that some small mission-driven institutions are unable to offer online checking and payment services to customers, accept online loan applications, conduct automated underwriting, or submit data electronically. For this reason, the NCUA provides technical assistance grants to eligible credit unions to support increased technological capacity and train support staff. Nevertheless, the costs to adopt technologies, which must also be updated continually to mitigate cybersecurity risk vulnerabilities, are likely to continue increasing.

Darryl E. Getter, Specialist in Financial Economics
Paul Tierno, Analyst in Financial Economics

IF12665

Disclaimer