NCUA
National Credit Union Administration

Third-Party Vendor Authority

March 2022

NCUA

National Credit Union Administration

Third-Party Vendor Authority

Third-Party Vendor Authority i
Executive Summary 1
Background 3
Risks 5
Technology Service Providers 7
CUSOs 7
Limitations in the NCUA's Authority 9
Conclusion 10
Appendix A: Timeline 11
Appendix B: Credit Union Service Organizations 15
Appendix C: Past Examples of Risks Associated with Third-Party Services 16
Appendix D: Draft Language – Federal Credit Union Act 18
Appendix E: Material Loss Reviews Associated with CUSOs 19

Executive Summary

This paper outlines significant risks and challenges presented by the National Credit Union Administration's (NCUA) lack of authority over third-party vendors that provide services to federally insured credit unions (FICU). This growing regulatory blind spot has the potential to trigger cascading consequences throughout the credit union industry and the financial services sector that may result in significant losses to the National Credit Union Share Insurance Fund (NCUSIF). Furthermore, third-party vendors may pose a national security risk to the United States due to a lack of oversight and enforcement authority over their business operations—mainly with respect to cybersecurity given the amount and type of data they hold, as well as business functions they perform for FICUs, with which roughly one in three Americans have a financial relationship.

The NCUA is seeking the *restoration* of statutory authority over third-party vendors, including credit union service organizations (CUSO). Specifically, the NCUA is seeking examination and enforcement authority over CUSOs, whether wholly or partially owned by FICUs; and examination authority over third-party service providers (also known as vendors throughout this paper). In reinstating the authority granted to the NCUA in the Examination Parity and Year 2000 Readiness for Financial Institutions Act (Examination Parity Act), the NCUA would obtain authorities similar to federal banking regulators under the Bank Service Company Act.

The adoption of the recent CUSO final rule on October 27, 2021, heightened the need for the NCUA to obtain vendor authority. The rule expands the list of permissible activities and services CUSOs provide to credit unions, including originating any loan that a federal credit union may originate. Yet, the NCUA's authority to regulate or supervise CUSOs has remained unchanged. To date, the NCUA cannot directly enforce access or initiate corrective action. As stated in the final rule, the NCUA Board's continuing policy is to seek third-party vendor authority from Congress.

Credit unions partner with third-party vendors to enhance the products and services provided to their members. These partnerships can make programs cost-effective, enable credit unions to access expertise, and promote programs that may not be feasible if provided independently. The pandemic accelerated the industry's movement to digital services, increasing credit unions' reliance on third-party vendors.

However, these relationships can pose various risks to credit unions. Outsourcing control over one or more business functions (many of which are fundamental operations for a financial institution) to a third-party increases the risks inherent in those functions, such as website management, loan underwriting, and payments processing, among others. Additionally, the

NCUA's lack of statutory authority to examine third-party vendors increases the risk that operational or financial problems can cascade through the credit union industry and the broader financial system. For example, as cyber actors continue to target third-party vendors, a failure or disruption of a critical third-party vendor that severely impacts the credit union system could affect the broader financial sector—including runs on other financial institutions. Without examination and enforcement authority, the NCUA has limited ability to determine the risk these relationships pose and to intervene when necessary.

The NCUA's Inspector General, the Financial Stability Oversight Council, and the Government Accountability Office have all called for the *restoration* of the NCUA's authority over CUSOs and third-party vendors. The NCUA Office of Inspector General (OIG) 2019 Report, *NCUA's Examination and Oversight Authority over Credit Union Service Organizations and Vendors*, recommends NCUA management continue its efforts to work with appropriate Congressional committees regarding amending the Federal Credit Union Act to grant the NCUA the authority to subject credit union service organizations and credit union vendors to examination and enforcement authority to the same extent as if they were an insured credit union.

Since 1999, the Government Accountability Office (GAO) has published three reports recommending that NCUA receive third-party vendor authority. In addition, since 2015, the Financial Stability Oversight Council's Annual Report (FSOC) has included the recommendation in every Annual Report that NCUA be given vendor authority; the FSOC 2020 Annual Report recommends that Congress pass legislation that ensures the NCUA has adequate examination and enforcement powers to oversee third-party service providers.

The NCUA has previously addressed this lack of authority before Congress during numerous hearings as outlined in Appendix A.

If the NCUA receives vendor authority, the agency would adopt a program that prioritizes exams based on risk to the NCUSIF, consumers, Bank Secrecy Act (BSA)/Anti-Money Laundering (AML), national security, and cybersecurity.

Background

Credit unions rely on third parties, including credit union service organizations (CUSO), for a range of products, services, and activities.[1] These may include core data processing, information technology services, accounting, compliance, and loan underwriting and servicing. A credit union may also use a third-party's platform to offer products and services to improve members' access to services. Use of third parties may also enable credit unions to access specific capabilities or expertise that would be difficult to provide in-house. To be competitive, credit unions take advantage of the benefits third parties provide and are increasingly transferring core business functions to CUSOs and other third-party vendors.

CUSOs offer additional benefits to credit unions and their members. First, credit unions may use economies of scale to lower operational costs. Instead of multiple credit unions providing and supporting a service individually, a CUSO arrangement creates cost efficiencies, particularly if it engages multiple credit unions. CUSOs also offer investment and ownership opportunities for credit unions, which can help increase credit union oversight of third parties and increase earnings. Fundamental activities, such as loan origination, lending services, and financial management are being outsourced to CUSOs.

The use of third parties can offer credit unions significant advantages, such as quicker and more efficient access to new technologies, delivery channels, products, services, and markets. However, under this approach, activities fundamental to the credit union mission, such as loan origination, lending services, compliance with Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) regulations, and financial management, are being outsourced to entities outside of NCUA's regulatory oversight.

Competition, advances in technology, and innovation in the financial sector contribute to the increasing use of third parties to perform business functions, deliver support services, and provide new and existing products and services. The COVID-19 pandemic has also increased credit union reliance on third parties by accelerating the industry's movement to digital services.

Although the services that third parties provide may offer associated benefits, those benefits should not come at the expense of reauthorizing vendor authority. Restoring the NCUA authority to examine third-party vendors would help smaller credit unions by providing valuable information for them to conduct due diligence on service providers. Credit unions are member-

[1] See Appendix B for more information on the difference between CUSOs and other third-party vendors.

owned, and many credit unions are small, with volunteer-based boards. Many of these volunteers and small credit unions do not possess the clout and subject matter expertise necessary to fully monitor their service providers. NCUA reviews can add value to the credit union system and a measure of assurance to improve the effectiveness of credit union due diligence efforts.

Risks

Outsourcing services, especially core business functions, affects various risk areas including national security, cybersecurity, concentration, reputation, compliance, and systemic and strategic risks, as described below.

- **National Security Risk**: Third-party vendors pose a national security risk to the United States due to a lack of oversight of their business operations—mainly with respect to cybersecurity given the amount and type of data they hold, as well as business functions they perform for credit unions. Credit unions are a major pillar of our national economic system and are an essential component of our national financial services critical infrastructure. Roughly one in three Americans have a financial relationship with a credit union, and a cyberattack by a retaliating or adversarial nation-state pose political instability—among other—risks within the United States by potentially cutting off millions, or tens of millions, of credit union members from their financial livelihoods and undermining the United States' national economic security. See additional risks in Technology Service Providers and Cybersecurity risks below. Additional information on this risk would be provided in a classified setting by appropriate agencies.

- **Cybersecurity Risk**: The NCUA is concerned about cyberattacks within the financial system. Cybercriminals and adversarial nation-states continue to focus their efforts on exploiting vulnerabilities identified across U.S. infrastructure sectors, including those of third-party service providers of information technology services. For example, as cyber actors continue to target third-party vendors, a failure or disruption of a critical third-party vendor that severely impacts the credit union system could affect the broader financial sector. Without examination and enforcement authority, the NCUA cannot determine the risks posed, intervene when necessary, or alert other appropriate federal agencies. The "Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers" notice of proposed rulemaking by the Federal Deposit Insurance Corporation (FDIC) requires notification of incidents that may materially affect the viability of a banking organization's operations, its ability to deliver banking products and services, or the stability of the financial sector of any significant computer security incident, no later than 36 hours after the organization determines that a cyber incident has occurred. For example, this includes large-scale distributed denial of service (DDoS) attacks that disrupt customer access to banking services, or computer hacking incidents that disable banking operations for extended periods of time. No similar cyber incident reporting requirements exist for credit union service providers. This is a gap that the NCUA needs to close with third-party vendor authority.

- **Concentration Risk**: Concentration risk is a significant concern, given that credit unions rely on many of the same vendors. A disruption or failure of a critical third party has the potential to impact hundreds of credit unions, causing financial losses and operational disruptions that can result in significant losses to the NCUSIF.

- **Systemic Economic Risk to the Financial Services Sector**: Since the NCUA does not have authority over third-party vendors, the NCUA relies upon the federal banking agencies to respond to a crisis at a third party. However, when there is an incident at a third-party that only services credit unions, the federal banking agencies do not have regulatory authority.[2] Therefore, neither the NCUA nor the banking agencies receive notification of the incident and would be unable to determine the impact on the entire financial sector or take timely remedial action. This event would have the potential to cause cascading consequences throughout the financial sector.

- **Reputation Risk**: Errors, delays, or omissions in information technology that become public knowledge or directly affect customers can significantly affect the reputation of the serviced financial institutions.

- **Compliance Risk**: Outsourced activities failing to comply with legal or regulatory requirements can subject the institution to legal sanctions. For example, inaccurate or untimely consumer compliance disclosures or unauthorized disclosure of confidential customer information could expose the institution to civil money penalties or litigation.

- **Strategic Risk**: Inadequate management experience and expertise leads to a lack of understanding and control of key risks. Additionally, inaccurate information from third parties can cause the management of serviced financial institutions to make poor strategic decisions.

The NCUA faces significant challenges associated with its lack of authority to examine third-party vendors. These challenges include the NCUA's limited ability to:

- Determine system-wide risks to the credit union industry caused by third-party vendors;

[2] As discussed in more detail in Appendix B, because CUSOs primarily serve credit unions and credit union members, they are generally outside the examination authority of the federal banking agencies.

- Identify risks a vendor poses to credit unions and the related potential impact to the NCUSIF and national economic security;
- Require CUSOs to implement corrective action outside of requiring a credit union to divest its ownership interest or any loan;
- Provide investing credit unions with due diligence related information about a vendor's operations and management;
- Assess or respond to systemic events that impact the financial sector;
- Participate in reviews of major vendors used by both credit unions and banks; and
- Determine vendor compliance with applicable laws and regulations.

Technology Service Providers

Credit unions increasingly outsource technology services to third-party vendors known as technology service providers (TSP). These types of third-party providers pose a unique risk to the credit unions. A credit union outsourcing its technology services can increase operational and information security risks. Operational risks include operations and transaction processing, network security, member service reliability, systems development and support, internal control processes, contingency planning, and consumer privacy. Over time, there has also been a consolidation of TSPs, which increases the concentration risk for the credit union system. As of September 30, 2021, the top five credit union core processing system third-party vendor categories (data processing, audit, eWeb, account verification, and Bank Secrecy Act) provide service to credit unions holding approximately 87 percent of total credit union system assets.

When there is an incident at a third party that only services credit unions, such as a CUSO, the federal banking agencies do not have regulatory authority. Therefore, neither the NCUA nor the banking agencies receives notification of the incident, and both would be unable to determine the impact of the incident on the entire financial sector and take timely remedial action.

CUSOs

CUSOs generally do not fall under the examination authority of the federal banking agencies. However, the Consumer Financial Protection Bureau has requisite authority to examine CUSOs to determine whether consumer protection laws are being followed. Because credit unions can invest in and lend to CUSOs, the failure of a CUSO can directly impact the financial condition of one or multiple credit unions, in addition to the operational disruptions that could occur from the loss of core business functions.

While there are many advantages to CUSOs, the concentration of credit union services presents a risk to the safety and soundness of the credit union industry by introducing systemic risk.

As of December 31, 2020, there were 992 registered CUSOs, including 50 CUSOs owned by corporate credit unions. At the end of 2020, approximately 93 percent of credit unions engaged the services of at least one CUSO, which represented more than 98 percent of total credit union system assets.

Additionally, the NCUA's OIG stated that between 2008 and 2015, nine CUSOs contributed to material losses to the NCUSIF. The report noted one of the CUSOs caused losses in 24 credit unions, some of which failed.[3] According to NCUA staff calculations, at least 73 credit unions incurred losses between 2007 and 2020.

As important as it is for credit unions to form strategic alliances within the credit union system, the migration of operations to CUSOs reduces the NCUA's ability to assess risk, ensure effective risk management, and enforce consumer financial protections and anti-money laundering requirements.

The NCUA has no authority to enforce vendor compliance with federal consumer financial protection laws and regulations nor compliance with prudential standards like concentration limits, maximum loan-to-value ratios, and minimum capital levels. The recent CUSO final rule also gives CUSOs the ability to become indirect auto and payday lenders. These two consumer financial products carry considerable compliance and reputational risk. Furthermore, the NCUA has limited visibility and no enforcement authority over CUSO lending abuses without third-party vendor authority. Third-party risks continue to be an area of heightened supervisory focus for the NCUA. Still, the lack of third-party vendor authority creates growing blind spots in the NCUA's supervision program.

[3] See OIG Report #OIG-07-20, *Audit of The NCUA's Examination and Oversight Authority Over Credit Union Service Organizations And Vendors.*

Limitations in the NCUA's Authority

While the NCUA issued guidance on due diligence in selecting and managing risk related to third-party vendors, the NCUA does not have authority to examine these vendors or enforce compliance with regulations in either CUSOs or third-party service providers.

In March 1998, Congress enacted the Examination Parity Act giving the NCUA Board temporary authority over CUSOs and third-party vendors to address Y2K readiness in the credit union industry. This authority expired on December 31, 2001. The NCUA has not had direct statutory authority over CUSOs or vendors for more than 20 years— during which the risks inherent to outsourcing critical financial services operations have grown and changed significantly.

After the Examination Parity Act expired, the NCUA continued to participate informally in the Federal Financial Institutions Examination Council (FFIEC) interagency supervisory program for reviewing technology service providers. The program, termed the Significant Service Provider (SSP) program, conducts examinations of technology service providers delivering mission-critical applications for large numbers of financial institutions regulated by more than one agency. The SSP reduces supervisory duplication by promoting effective use of agency resources and reducing the burden on technology service providers while producing a single examination report for the technology service provider and its associated financial institutions. The SSP enables the federal financial agencies to share their knowledge of technology service providers' operations and to develop a joint supervisory strategy. However, in 2016, the federal banking agencies discontinued the NCUA's participation in SSP program examinations because the NCUA is not statutorily authorized to conduct examinations on third-party vendors. The NCUA's ability to evaluate risk in credit union vendors by leveraging the banking agencies' authorities is now very limited.

The NCUA previously attempted to address this issue without resorting to legislative changes by requesting that third-party vendors voluntarily allow NCUA reviews. Until 2013, the NCUA conducted third-party vendor reviews on a voluntary basis. Several vendors declined the NCUA's examination requests for voluntary examinations, and other vendors rejected the NCUA's recommendations to implement corrective actions to mitigate identified risks. For example, several vendors *refused* to implement the NCUA's recommendations to improve network security and safeguard sensitive member information. These scenarios impact the NCUA's ability to address the risk third-party vendors and CUSOs pose to the credit union industry and the broader financial system.

Currently, the NCUA has limited ability to provide direct oversight over the services provided by CUSOs, which include many core business functions. The NCUA does have access to a CUSO's books and records and the ability to review the CUSO's internal controls through contractual language credit unions are required to have with the CUSO; however, the NCUA does not have the ability to directly enforce this access or to initiate corrective action. The NCUA only has limited and insufficient authority, through the credit union investors, to require corrective action of any identified deficiencies in the operation of CUSOs. While the NCUA can assess the credit union's ability and performance in managing the relationship with the CUSO, the NCUA may have limited access to the people, processes, and procedures related to the services being performed by the CUSO.

Conclusion

Credit unions use CUSOs and third-party vendors to support their operational structure, enhance their business model, and provide products and services to members. The rapid acceleration into new products and services through deployment of new and innovative technology will continue to attract credit unions to CUSOs and third-party service providers that license and implement innovative services. This results in a growing regulatory blind spot for the NCUA under current statutory limitations. Without the statutory authority to examine third parties and enforce corrective actions for CUSOs, the NCUA is limited in its ability to protect the NCUSIF. Moreover, the NCUA is also limited in its ability to provide federal insight into risks posed to our national economic system through its work in the Financial and Banking Information Infrastructure Committee and in its ability to protect consumers and the overall health of the broader credit union system, which is a major pillar of the American economy and national financial system.

If the NCUA's vendor authority is restored, the agency will adopt a program that prioritizes examinations based on risk to the NCUSIF, consumers, BSA/AML, national economic security, and cybersecurity. While this may increase the NCUA's budget due to the addition of more examiners with specific expertise, the agency does not expect a dramatic increase that will impact the operations of credit unions. If vendor authority is reauthorized, NCUA will once again be able to leverage the work of federal banking agency partners to minimize costs.

Appendix A: Timeline

Year	Activity
2021	The NCUA Chairman Todd Harper's May 2021 testimony to Congress addressed the NCUA's lack of vendor authority. The NCUA Chairman Todd Harper's August 2021 testimony to Congress addressed the NCUA's lack of vendor authority. FSOC 2021 Annual Report states that the NCUA continues to have no authority to supervise CUSOs for compliance with federal consumer financial protection laws and regulations, the Bank Secrecy Act and other anti-money laundering laws, or with prudential standards. The report also recommends that Congress pass legislation that ensures that NCUA and other relevant agencies have adequate examination and enforcement powers to oversee third-party service providers.
2020	The International Monetary Fund supported the FSOC recommendation to enhance third-party service provider information security (2020 Financial Sector Stability Assessment Paper of the United States). FSOC 2020 Annual Report recommends that Congress pass legislation ensuring the NCUA have adequate examination and enforcement powers to oversee third-party service providers. NCUA Office of Inspector General, Audit of the NCUA's Examination and Oversight Authority over Credit Union Service Organizations and Vendors recommends that the NCUA management continue its efforts to work with appropriate Congressional committees regarding amending the FCU Act to grant the NCUA the authority to subject CUSOs and vendors to examination and enforcement authority to the same extent as if they were an insured credit union.

Year	Activity
2019	The NCUA Chairman Rodney E. Hood's May 2019 testimony to Congress addressed the NCUA's lack of vendor authority. FSOC 2019 Annual Report recommends that Congress pass legislation ensuring that the NCUA has adequate examination and enforcement powers to oversee third-party service providers.
2018	The NCUA Chairman Mark McWatters' October 2018 testimony to Congress addressed the NCUA's lack of vendor authority. FSOC 2018 Annual Report recommends that Congress pass legislation ensuring that the NCUA have adequate examination and enforcement powers to oversee third-party service providers.
2017	FSOC 2017 Annual Report recommends Congress pass legislation that grants examination and enforcement powers to the NCUA to oversee third-party service providers.
2016	FSOC 2016 Annual Report supports granting examination and enforcement powers to the NCUA to oversee third-party service providers, including information technology, and more broadly, other critical service providers engaged with credit unions.

Year	Activity
2015	GAO recommended that Congress modify the FCU Act to grant NCUA authority to examine technology service providers of credit unions to ensure that NCUA has adequate authority to determine the safety and soundness of credit unions (GAO-15-509 Cybersecurity: Bank and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Usable Threat Information). The NCUA Director of the Office of Examination and Insurance, Larry Fazio, addressed the NCUA's lack of vendor authority in his April 2015 testimony to Congress. FSOC 2015 Annual Report supports the granting of examination and enforcement powers to oversee third-party service providers engaged with credit unions.
2011	The NCUA Chairman Debbie Matz's June 2011 testimony to Congress addressed the NCUA's lack of vendor authority.
2010	The NCUA Chairman Debbie Matz's December 2010 testimony to Congress addressed the NCUA's lack of vendor authority.
2004	The NCUA Chairman Joann Johnson's June 2004 testimony to Congress addressed the NCUA's lack of vendor authority.
2003	GAO recommended Congress consider granting NCUA legislative authority to examine third-party vendors that provide services to credit unions and are not examined through FFIEC (GAO-04-91 Credit Union Financial Condition).
2001	The NCUA's authority to examine third-party vendors under the Examination Parity Act ended on December 31, 2001.

Year	Activity
1999	The Examination Parity Act temporarily gave the NCUA examination and regulatory authority over vendors, similar to the other federal banking agencies. The GAO recommended Congress consider whether NCUA’s authority to examine the performance of services provided to credit unions by third-party firms is needed to ensure the safety and soundness of credit unions and should be extended beyond December 31, 2001 (GAO/GGD-99-91 Enhancing Oversight of Internet Banking).
1962	The Bank Service Company Act (12 U.S.C. § 1867), provides the federal banking agencies with authority to regulate and examine a bank service company.

Appendix B: Credit Union Service Organizations

CUSOs are a type of third-party provider unique to credit unions. Under the FCU Act, a credit union organization is defined as any organization, as determined by the Board, which is established primarily to serve the needs of its member credit unions, and whose business relates to the daily operations of the credit unions they serve.[4] A CUSO is an entity structured as a corporation, limited liability company, or limited partnership at the individual state level.[5] These organizations provide services on a wholesale level to credit unions and/or on a retail level to credit union members. Commercial or wholesale services are typically developed to provide greater efficiencies.

FICUs may not have sufficient levels of activity or enough expert resources to manage a specialized service area. The CUSO structure allows credit unions to pool resources and share expert resources and systems to achieve economies of scale comparable to other larger financial organizations. CUSOs provide a vital service to help credit unions provide competitive, quality services to members and operate efficiently. They also promote the flow of capital and liquidity throughout the system.

Over 90 percent of FICUs use CUSOs, and there is increasing interconnectedness between credit unions through CUSO operations. Moreover, the types and scope of services provided by CUSOs are diversifying to meet the institutions' and members' financial service needs. Currently, CUSOs are permitted to originate any type of loan that an FCU may originate. To mitigate risk, FCUs only have the authority to lend up to one percent of their paid-in and unimpaired capital and surplus, and to invest an equivalent amount, in total to CUSOs. Additionally, FICUs that obtain an ownership interest in a CUSO ensure by contract that the NCUA has access to the CUSO's books and records and other information and reports.

[4] 12 U.S.C. 1757(5)(D)

[5] Because CUSOs primarily serve credit unions and their members, they are often outside the examination authority of the federal banking agencies and are usually only subject to state supervision under the laws in the state where the CUSO is located.

Appendix C: Past Examples of Risks Associated with Third-Party Services

Example #1

Loan fraud tied to data processing concerns resulted in the largest natural-person credit union failure in history, a $170 million loss to the NCUSIF. The data processing system provider was a small vendor, which had 35 client credit unions. Credit union management hid fictitious loans through a mixture of actual and claimed system deficiencies. The data processing system had weaknesses in wire transfer monitoring reports required by the Bank Secrecy Act and the Office of Foreign Assets Control, helping to mask the primary mechanism for transferring the funds out of the country. These system deficiencies substantially slowed detection of the fraud, increasing the loss amount. When third-party vendors perform functions that include online banking, transaction processing, fund transfers, and loan underwriting, the data are being stored on these vendors' servers—which in some cases may be stored on foreign servers. In addition, vendors that process funds, such as shared branching networks, can create gaps in anti-money laundering oversight.

Example #2

A CUSO offers peer-to-peer and peer-to-merchant mobile payments, and new and emerging electronic banking services. The CUSO reported that it reached $1 million per day transaction volume with rapid growth and is targeting $1 billion annually.

The NCUA has concerns about the rapid growth rate, insurability of the deposited funds, Bank Secrecy Act compliance, and whether the mobile payments application complies with FFIEC authentication guidance. The potential exposure is currently unknown.

Example #3

A credit union contracted with a third party for passing through first mortgage applications. The credit union encountered problems with the third party purchasing the loans in a timely manner. Under the contract, the third party (responsible for underwriting the loan) was to purchase loans within 30 days. These were loans that the credit union funded and sent to the third party. Funds repaying the credit union for these loans were never received and had been diverted.

Example #4

This CUSO underwrites and services loans for several local credit unions. Past activity was substandard, and a large portion of the serviced portfolio came to be owned by one FICU that could not recover from the CUSO's poor lending practices. Loan losses in both the commercial and consumer loan portfolios resulted in the credit union's ultimate merger.

Appendix D: Draft Language – Federal Credit Union Act

Repeal of 2001 Sunset of NCUA Third-Party Authority

REGULATION AND EXAMINATION OF CREDIT UNION ORGANIZATIONS AND SERVICE PROVIDERS. Section 206A of the Federal Credit Union Act (12 U.S.C. 1786a) is amended—

(1) in subsection (a)(1), by striking ‘‘that’’ and inserting ‘‘an’’;

(2) in subsection (c)(2), by inserting after ‘‘shall notify the Board’’ the following: ‘‘, in a manner and method prescribed by the Board,’’; and

(3) by striking subsection (f).

Appendix E: Material Loss Reviews Associated with CUSOs

Material Loss Reviews Associated with CUSOs (as of December 31, 2021):

Report No.	Title	Date
OIG-17-05	Material Loss Review of Chester Upland School Employees, OPS EMP, Electrical Inspectors, Triangle Interest % Service Center, Cardozo Lodge, and Servco Federal Credit Unions	2/23/2017
OIG-13-10	Material Loss Review of Chetco Federal Credit Union	10/1/2013
OIG-13-05	Material Loss Review of Telesis Community Credit Union	3/15/2013
OIG-12-14	Material Loss Review of Eastern New York Federal Credit Union	11/19/2012
OIG-10-20	OIG Capping Report on Material Loss Reviews	11/23/2010
OIG-10-14	Material Loss Review of Clearstar Financial Credit Union	9/22/2010
OIG-10-15	Material Loss Review of Ensign Federal Credit Union	9/23/2010
OIG-08-10	Material Loss Review of Huron River Area Credit Union	11/26/2008