FERC–912 (IC22–9–000)—COGENERATION AND SMALL POWER PRODUCTION, PURPA SECTION 210(m) REGULATIONS FOR TERMINATION OR REINSTATEMENT OF OBLIGATION TO PURCHASE OR SELL

	Number of respondents	Number of responses per respondent	Total number of responses	Average burden hours & average cost per response ($) [4]	Total annual burden hours & total annual cost ($)	Cost per respondent ($)
	(1)	(2)	(1) × (2) = (3)	(4)	(3) × (4) = (5)	(5) ÷ (1) = (6)
Termination of obligation to purchase	4	1.5	6	12 $1,224	72 $7,344	$1,836
Reinstatement of obligations to purchase	0	0	0	0 $0	0 $0	0
Termination of obligation to sell	2	1	2	8 $816	16 $1,632	816
Reinstatement of obligation to sell	0	0	0	0 $0	0 $0	0
Total			8		88 hours $8,976	2,652

Comments: Comments are invited on: (1) whether the collection of information is necessary for the proper performance of the functions of the Commission, including whether the information will have practical utility; (2) the accuracy of the agency's estimate of the burden and cost of the collection of information, including the validity of the methodology and assumptions used; (3) ways to enhance the quality, utility and clarity of the information collection; and (4) ways to minimize the burden of the collection of information on those who are to respond, including the use of automated collection techniques or other forms of information technology.

Dated: September 10, 2026.

Debbie-Anne A. Reese,

Secretary.

[FR Doc. 2026–18872 Filed 9–14–26; 8:45 am]

BILLING CODE 6717–01–P

[4] The estimates for cost per response are derived using the following formula: Average Burden Hours per Response * $102.00 per Hour = Average Cost per Response. The hourly cost figure comes from the FERC average salary ($213,003/year). Commission staff believes the 2026 FERC average salary to be a representative wage for industry respondents.

FEDERAL RESERVE SYSTEM

[Docket No. OP–1880]

Proposed Third-Party Risk Management Guide for Traditional Community Banking Organizations

AGENCY: The Board of Governors of the Federal Reserve System (Board).

ACTION: Proposed guidance and request for comment.

SUMMARY: The Board invites comment on a proposed guide for traditional community banking organizations on managing risks associated with third-party relationships. The proposed guide would reflect the Board's supervisory experience and lessons learned through examining community banking organizations' third-party risk management practices. In particular, the proposed guide would discuss the key risks faced by traditional community banking organizations in their third-party relationships in general and in relation to particular categories of third-party relationships most common to traditional community banking organizations.

DATES: Comments must be received on or before November 16, 2026.

ADDRESSES: You may submit comments, identified by Docket No. OP–1880 by any of the following methods:

- *Agency Website: https://www.federalreserve.gov/apps/proposals/.* Follow the instructions for submitting comments, including attachments. *Preferred Method.*
- *Mail:* Benjamin W. McDonough, Secretary, Board of Governors of the Federal Reserve System, 20th Street and Constitution Avenue NW, Washington, DC 20551.
- *Hand Delivery/Courier:* Same as mailing address.
- *Other Means: publiccomments@frb.gov.* You must include docket number in the subject line of the message.

Comments received are subject to public disclosure. In general, comments received will be made available on the Board's website at *https://www.federalreserve.gov/apps/proposals/* without change and will not be modified to remove personal or business information including confidential, contact, or other identifying information. Comments should not include any information such as confidential information that would be not appropriate for public disclosure. Public comments may also be viewed electronically or in person in Room M–4365A, 2001 C St. NW, Washington, DC 20551, between 9 a.m. and 5 p.m. during Federal business weekdays.

FOR FURTHER INFORMATION CONTACT: Juan Climent, Deputy Associate Director, (202) 460–2180, Jeff Ernst, Manager, (202) 369–9439, Allison Boller, Sr., Financial Institution Policy Analyst II, (202) 253–4686, Joseph Vall-Llobera, Director of Examinations, (470) 733–1198, Division of Supervision and Regulation; or Claudia Von Pervieux, Special Counsel, (202) 469–1020, Benjamin Nuyens, Senior Counsel, (202) 909–7574, Legal Division; Board of Governors of the Federal Reserve System, 20th Street and Constitution Avenue NW, Washington, DC 20551.

SUPPLEMENTARY INFORMATION:

I. Overview

As described elsewhere in today's **Federal Register**, the Board, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the National Credit

Union Administration (collectively, the ''agencies'') published for comment proposed guidance on third-party risk management that would apply to all banking organizations supervised by the agencies, *Proposed Third-Party Risk Management Guidance* (Proposed All-Bank TPRM Guidance). The Proposed All-Bank TPRM Guidance would provide principles for banking organizations to consider when managing third-party risks.

Some community banks have expressed the need for additional resources to support their third-party risk management efforts. To address that need, the Board is issuing for comment a proposed guide on third-party risk management for ''traditional community banking organizations'' [1] (Community Bank Guide) that is intended to serve as a companion document to the Proposed All-Bank TPRM Guidance. The proposed Community Bank Guide would have the explicit goal of assisting TCBOs in understanding and conducting third-party risk management. It would articulate how the principles in the Proposed All-Bank TPRM Guidance can be applied in practice by TCBOs. Limiting the scope to TCBOs and the third parties they tend to engage with makes it possible to provide clear examples of how smaller banking organizations can operationalize the high-level principles in the Proposed All-Bank TPRM Guidance.

The proposed Community Bank Guide would not be relevant to other institutions, as it would be specifically tailored to the unique characteristics and risk profiles of TCBOs. It would not be a rule, and banking organizations would not be required to take the actions described in the guide.

The Board seeks comment on whether the proposed Community Bank Guide would be useful to TCBOs and how it could be improved. In particular, the Board is interested in feedback on whether the proposed guide provides the appropriate level of detail, such that it will serve as a useful resource for TCBOs without establishing *de facto* supervisory standards.

In drafting the proposed Community Bank Guide, the Board has endeavored to distill the key risks and risk management considerations associated with third-party relationships most engaged in by TCBOs. In doing so, the Board consulted various resources, including relevant sections of examination materials (*e.g.,* the Federal Financial Institutions Examination Council's *IT Examination Handbook* and *Bank Secrecy Act/Anti-Money Laundering Examination Manual*), industry materials, and responses to the agencies' relevant requests for information.[2] The Board also used information learned from the supervisory process, including sound risk management practices the Board has seen at TCBOs (including associated materials such as risk assessment methodologies, sample contracts, and due diligence files).

II. Request for Comment

The Board invites comment on all aspects of the proposed Community Bank Guide. The Board also seeks feedback on ways to improve upon the proposed guide so that it can be as useful as possible for TCBOs in managing their third-party risks. In addition, the Board invites comment on these specific topics:

- What are the advantages and disadvantages of tailoring the expectations established in the proposed Community Bank Guide to banking organizations with assets below $30 billion?
- How, if at all, could the Board further clarify the characteristics of a TCBO? What additional examples of community banking organization profiles, if any, would be helpful to clarify whether a community banking organization would be within the scope of the proposed Community Bank Guide?
- The proposed guide is meant to serve as a resource for TCBOs to support their efforts to manage risks from third-party relationships. To what extent would the information included in the proposed guide be useful for TCBOs? How can the proposed guide be clarified or modified to advance that objective?
- In drafting the proposed guide, the Board sought to provide a level of detail that would make the document a useful practical resource. At the same time, the Board sought to avoid creating *de facto* standards that TCBOs believe they would be evaluated against. To what extent has the Board appropriately calibrated the level of detail in the proposed guide?
- What changes or additional clarifications, if any, would be helpful regarding the overarching third-party risk management considerations used by TCBOs, provided in Section IV.B?
- What adjustments should the Board consider to the proposed categories of vendor types most used by TCBOs? What additional categories, if any, should Section IV.C provide?
- How can the proposed guide be improved to better support contract negotiations with third parties?
- Should ''deposit placement networks'' be included as an additional vendor category in Section IV.C? Would TCBOs benefit from having specific third-party risk management considerations for this type of relationship? If so, how do the overarching risk management considerations apply and what additional risk considerations are most relevant?

III. Paperwork Reduction Act

The Paperwork Reduction Act of 1995 (44 U.S.C. 3501–3521) (PRA) states that no agency may conduct or sponsor, nor is the respondent required to respond to, an information collection unless it displays a currently valid Office of Management and Budget (OMB) control number.

The guide does not revise any existing, or create any new, information collections pursuant to the PRA. Rather, any reporting, recordkeeping, or disclosure activities mentioned in the guide are usual and customary and should occur in the normal course of business as defined in the PRA.[3] Consequently, no submissions will be made to the OMB for review.

IV. Text of Proposed Third-Party Risk Management Guide for Traditional Community Banking Organizations

[1] ''Traditional community banking organizations'' (''TCBOs'') are banking organizations with less than $30 billion in assets that focus on serving their local communities. The proposed guide is not intended for community banking organizations with more complex business models or third-party relationship profiles, such as complex bank-fintech partnerships (*e.g.,* where a bank makes products or services available through an arrangement with one or more fintech companies and the fintech company, rather than the bank, markets, distributes, or otherwise provides access to the products or services).

[2] ''Request for Information on Bank-Fintech Arrangements Involving Banking Products and Services Distributed to Consumers and Businesses,'' 89 FR 61577 (July 31, 2024); ''Request for Information Regarding Community Bank Digitalization,'' 90 FR 20212 (May 12, 2025); and ''Request for Information Regarding Community Banks' Engagement With Core Service Providers and Other Essential Third-Party Service Providers,'' 90 FR 54882 (November 28, 2025).

[3] 5 CFR 1320.3(b)(2).

4. Payment Processing and Digital Banking Providers
5. Loan Management System Providers
6. Card Issuing and Processing Providers
7. BSA/AML and Financial Crime Platform Providers
8. Fraud Prevention and Detection Providers

A. Introduction

Community banking organizations regularly rely on third parties [4] to support their banking operations. Third-party relationships can offer community banking organizations access to new technologies, risk-management tools, human capital, delivery channels, products, services, and markets. The Board of Governors of the Federal Reserve System (''Board'') is issuing this guide to provide a resource for traditional community banking organizations in managing risks that arise from their third-party relationships. For purposes of this guide, ''traditional community banking organizations'' (''TCBOs'') are banking organizations with less than $30 billion in assets that focus on serving their local communities.[5] For the purposes of this guide, consumer compliance is not in scope.

This guide complements the proposed guidance described elsewhere in today's **Federal Register**, *Proposed Third-Party Risk Management Guidance,* which applies to all banking organizations supervised by the agencies (All-Bank TPRM Guidance). This guide is an additional resource for TCBOs supervised by the Board and helps explain how such institutions could operationalize the principles articulated in the All-Bank TPRM Guidance.

This guide is divided into two main sections. The first section discusses four overarching third-party risk management topics, which are common to the types of third-party relationships [6] that TCBOs typically engage with:

- *Operational Resilience:* How a third party's operational disruptions could affect a TCBO.
- *System and Information Security:* A third party's impact on the security of a TCBO's sensitive networks, systems or data.
- *Compliance with Rules and Regulations:* How a third party impacts a banking organization's compliance with applicable rules and regulations.
- *Financial Resilience:* The impact of a third party's financial standing on a TCBO.

The second section identifies eight categories of third parties that smaller banking organizations often engage with, namely, core service providers, information technology infrastructure providers, cybersecurity providers, payment processing and digital banking providers, loan management system providers, card issuing and processing providers, Bank Secrecy Act/Anti-Money Laundering (BSA/AML) and financial crime platform providers, and fraud prevention and detection providers. For each third-party type, this guide discusses (1) how the overarching considerations discussed in the first section apply; and (2) additional risk management considerations specific to the third-party category. In the case of certain categories, this guide also includes a discussion of risk management strategies a TCBO may consider when transitioning to a new provider.

There are many ways to manage third-party risks effectively, and the suggestions in this guide are not the only available practices for TCBOs to effectively manage their risks. There is no one-size-fits-all approach to effective risk management. The examples and details in this guide are intended to support TCBOs in establishing appropriate third-party risk management practices. This guide does not set forth enforceable standards or prescriptive requirements; accordingly, non-compliance with this guide will not by itself result in supervisory criticism against a banking organization.[7] Additionally, each banking organization is responsible for operating in a safe and sound manner and adopting risk management practices that are best suited to managing the specific risks that it faces. All examples and risk considerations in this guide are illustrative, are not comprehensive, and will not be applicable to all situations.

B. Overarching Third-Party Risk Management Considerations

This section discusses four third-party risk management topics that will generally be the highest priority for TCBOs. For each topic, it provides overarching risk management considerations.

1. Operational Resilience

A TCBO typically has several third-party relationships that are essential to its operations, such that if the vendor experiences a serious disruption, the TCBO would struggle to operate. With this degree of reliance, the TCBO's operational resilience depends to a large degree on the operational resiliency of the third party. As a result, assessing the operational resilience of such third parties may be a high priority for the TCBO.

A third party's operational resilience can become compromised in any number of ways, such as cyberattacks and information technology failures. A TCBO is generally not expected to have the technical expertise to assess such risks itself. It may, therefore, rely on a review of reasonably conducted independent assessments for the matters covered therein, such as:

- SSAE 18 SOC Reports (Statement on Standards for Attestation Engagement Service Organization Control Reports);
- Technology service provider reports from the Federal banking agencies (if applicable);
- Audit reports;
- Penetration testing reports;
- Industry standard assessments (*e.g.,* Payment Card Industry Data Security Standard (PCI DSS), National Institute of Standards and Technology (NIST), and International Organization for Standardization (ISO)).

Additionally, as part of due diligence, contract negotiation, and monitoring, a TCBO may consider the third party's historical system uptime performance, service availability metrics, and whether performance capabilities align with the TCBO's needs. This may involve reviewing the results of business continuity/disaster recovery tests in light of the TCBO's recovery time and recovery point objectives. To facilitate this review, it is useful for contracts to address a TCBO's right to access these reports, or the right to audit directly if reports are unavailable.

A TCBO may also seek to negotiate service level agreements (SLAs) for operational resiliency in contracts with third parties (*e.g.,* system availability commitments and cyber incident notification requirements) and monitor for compliance against the SLAs. The Board recognizes that a TCBO may lack leverage in contract negotiations with

[4] For the purposes of this document, the term ''third party'' is interchangeable with ''service provider'' and ''vendor.''

[5] This guide is not intended for community banking organizations with more complex business models or third-party relationship profiles, such as complex bank-fintech partnerships (*e.g.,* where a bank makes products or services available through an arrangement with one or more fintech companies and the fintech company, rather than the bank, markets, distributes, or otherwise provides access to the products or services).

[6] A third-party relationship is defined in the All-Bank TPRM Guidance as a business arrangement between a banking organization and an entity or individual for the provision of one or more products, services, and other activities that support the banking organization.

[7] *See* 12 CFR part 262, Appendix A. However, supervisory action may result for any violations of law or unsafe or unsound practices stemming from insufficient management of third-party risk.

certain third parties, and may not be able to obtain optimal terms.[8]

2. System and Information Security

Third-party relationships can also complicate a TCBO's efforts to protect sensitive systems, data, and information. Third parties often need access to sensitive banking organization systems to provide their services. While granting this access can allow a TCBO to benefit from the third party's services, it can also create new vulnerabilities to cyberattacks. A third party's interaction with a banking organization's systems and information creates a new ''attack vector'' that can be exploited. Security incidents at vendors could lead to the theft of banking organization customer data or compromise banking organization systems and may require regulatory reporting.[9]

Effective due diligence and ongoing monitoring of third parties with access to sensitive banking organization systems may include reviewing audit reports and other independent assessments that identify the design and operating effectiveness of controls that protect banking organization information. Independent assessments often include information on the type of sensitive data protected and the access controls, encryption, incident response, backup and disaster recovery processes and associated operational effectiveness. Independent assessments may also evaluate the third party's ability to identify unauthorized activity and suspicious patterns indicative of a party seeking to access sensitive information and the effectiveness of remediation activities if information is comprised.

Contracts may address access to audits and other relevant reports, and a third party's responsibility for notifying the TCBO of cybersecurity incidents and remediation, including acceptable reporting timelines. A TCBO may also consider negotiating for liability provisions for security breaches, data loss, and regulatory violations resulting from vendor security failures and requirements that vendors maintain insurance to cover costs associated with information security breaches, investigations, recoveries, and business interruption. A TCBO may benefit from monitoring cyber events that impact the vendor, and ongoing enhancements to the vendor's information systems control environment.

When terminating a relationship with a vendor that has access to sensitive systems or data, a TCBO may benefit from verifying that the data has been successfully migrated or destroyed, that access has been removed, and that any continuing obligations (*e.g.,* transition assistance and log retention) are in place.

3. Compliance With Rules and Regulations

A TCBO's third-party relationships may have implications for its compliance with applicable rules and regulations, either because the third party performs a service on the TCBO's behalf that is subject to a compliance regime; or because the third party offers services that support the TCBO's compliance efforts. For example, use of a third-party BSA/AML system directly impacts a TCBO's ability to comply with BSA/AML laws. Meanwhile, a core service provider's ability to accurately store and transmit data can impact regulatory reporting requirements. Additionally, many TCBOs participate in payment networks, such as the National Automated Clearing House Association (NACHA) or card networks. These networks often maintain operating rules, and TCBOs may rely on third parties to help them comply with those rules. In such cases, third-party errors could leave a TCBO out of compliance with network rules, and lead to fines or in severe cases, loss of network access.

Due diligence and ongoing monitoring of third parties that provide services that support a TCBO's compliance efforts may include a review of negative news screens, compliance attestations, certifications of good standing from relevant entities, and independent audit reports to understand the third party's historical record of regulatory and rules compliance; quality and consistency of alerts, errors and exception reporting; and the third party's ability to incorporate regulatory changes into services. A TCBO may consider contractually identifying the third party's roles and responsibilities for supporting the TCBO's compliance with rules and regulations, including implementing timely regulatory changes, notification requirements, and responding to regulatory or TCBO customer inquiries, where applicable. Contracts may consider liability or indemnification provisions for network rules or regulatory violations caused by the third party, as well as access to audits or attestations that validate the third party's ability to comply with such rules and regulations. Where relevant, contracts can establish clear data retention obligations aligned with regulatory requirements.

Finally, a TCBO is ultimately responsible for compliance with rules and regulations and may benefit from tracking regulator or network rule changes that may have implications for the provider's services; and confirming the vendor makes any changes necessary to ensure compliance.

4. Financial Resilience

A third party's financial resilience can also be an important risk management consideration to the extent a TCBO relies on the third party for essential operations and the availability of substitutes. During due diligence and ongoing monitoring, a TCBO may approach evaluating the financial resilience of a third party in a manner consistent with the third party's risk profile. For example, a TCBO may limit a review of the third party's financial standing to publicly available information such as credit ratings, SEC filings, and market intelligence when the third party is a publicly-registered entity with established operating history. Conversely, when the third party is a private company or newer market entrant, a TCBO may benefit from a more concentrated assessment of the third party's financial standing. This may include reliance on funding sources, cash outlay, and *pro forma* financial statements, among other factors.

A TCBO may experience challenges in acquiring reliable or independently validated financial information from privately-owned third parties, including third parties in the startup phase. In such cases, the TCBO may choose to accept higher inherent risk or even be willing to contribute financially to the third party, depending on the distinct advantages it may offer. The TCBO may consider establishing contractual commitments for the third party to provide financial information at a future point in time, hold adequate levels of insurance, or limit growth of its services to the TCBO until financial performance can be adequately assessed.

C. TPRM Considerations on a Vendor-by-Vendor Basis

This section contains third-party risk management considerations for the third-party relationships most common to TCBOs. For each category, the guide explains how the overarching risk management considerations from

[8] This qualifier applies in all cases where the guide describes effective risk management principles for contract negotiation. As stated in the All-Bank TPRM Guidance, ''[t]he banking organization may still reasonably proceed with the relationship if, for example, the banking organization has a reasonable understanding of the risks relevant to the third-party relationship and any residual risks are in line with the banking organization's risk appetite and tolerances, especially if there are limited alternative options.''

[9] *See* 12 CFR part 208, App. D–2, 12 CFR part 225, subpart N.

Section IV.B apply, and then discusses additional risk management considerations that may be relevant. In some categories, the guide also discusses considerations for transitioning to a new third party.

1. Core Providers

Many TCBOs rely on core processing service providers (core providers) to develop and maintain the central system of record and operational backbone for TCBOs. These systems manage customer accounts, process daily transactions across deposits and loans, maintain the general ledger, generate regulatory reports, and serve as the integration hub connecting specialized applications. Generally, core providers are the most material and complex third-party relationship for TCBOs.

Overarching Risk Management Considerations

A core provider's availability, integrity, and security are essential to nearly all banking operations. Moreover, core providers often deliver multiple services beyond the core processing platform, such as payment processing, card programs, loan origination, or digital banking. Relying on a single provider for multiple services may offer operational efficiencies and simplified third-party risk management, but can also create heightened risk if the third party experiences financial distress, operational failures, or security compromises. For all these reasons, financial and operational resilience and system and information security are primary risk factors for a TCBO to consider when overseeing core provider relationships. In managing these risks, a TCBO may benefit from consulting the risk management strategies discussed in Section IV.B.

Specific Risk Management Considerations

Core systems can play an essential role in integrating various applications and platforms TCBOs rely on. For example, in order to operate effectively, BSA/AML and fraud detection systems must be able to communicate with payments, card, or loan processing systems. Such integration between a TCBO's systems can be essential to its operations. Integration failures can lead to significant operational breakdowns. To mitigate the risk of such failures, a TCBO may consider:

- testing integrations in a separate test environment, prior to going live;
- establishing contractual service agreements to maintain the security and availability of integrations; and
- monitoring performance of established connections and integrations, especially following material business or regulatory changes and through periodic continuity testing.

Given the core system's integration into a wide array of daily banking operations, monitoring can primarily occur through routine business practices that include system-generated alerts for failed transactions or processing errors. Daily reconciliation processes between connected systems provide inherent monitoring of core platform accuracy through ledger balancing, exception investigation, and researching if errors were appropriately captured and detected within the system. TCBOs may benefit from closely controlling for and resolving any ledger reconciliation issues prior to going live following a core conversion. Furthermore, when integrating new cores, other systems may require substantial migrations such as card or loan systems. Phasing these complex and resource intensive migrations over time can aid the TCBO in managing risk.

Core Conversion

The process of switching to a new core provider or platform is often referred to as a ''core conversion.'' A TCBO may consider a core conversion for a variety of reasons, including to:

- benefit from a more modern system that is more reliable and offers straightforward integration with other third parties;
- migrate from a platform being sunset or discontinued by the vendor;
- negotiate more equitable pricing and contract terms;
- gain greater control over the TCBO's own data; and
- obtain more responsive customer support (from the core to the TCBO).

These benefits, however, can come at a cost. Core conversions can be expensive and involve significant operational complexity. The Board supports TCBOs' pursuing modernization to meet customer needs and recognizes that TCBOs may reasonably accept higher risk when adopting technology-forward core systems that enable greater agility and innovation. The decision whether to undertake a core conversion is TCBO-specific. An individual TCBO must ultimately determine whether the benefits justify the risks and expense, based on its business model and risk tolerance. Many TCBOs benefit from specialized core conversion consultants or special counsel when undertaking a conversion.

As an alternative to full conversion, a TCBO may consider relying on an integration platform, often referred to as a middleware provider. Integration platform providers assist banking organizations when legacy core providers cannot facilitate integrations with desired products. An integration platform enables the flow of data between the TCBO's core and ancillary systems, and the systems of another third party. As an example, a TCBO may contract with a third party to offer a specific product that records transactions in a separate ledger. To pass transactional information back to the TCBO's core system, it chooses to contract with another third-party integration platform to establish Application Programming Interface (API) connections. Adding such a platform extends the value chain and presents different inherent risks than a conversion.

In addition to the factors discussed in Section IV.B, a TCBO deciding whether to undertake a core conversion and which provider to use may consider:

- direct and indirect costs of conversion, which may include licensing or subscription fees, implementation and conversion services, potential early termination fees for the existing provider, third-party consulting services, and internal staff time diverted from normal responsibilities;
- whether the prospective core provider will be able to meet the TCBO's evolving strategic needs, based on the provider's current and planned offerings;
- ease and cost of integration with other systems the TCBO relies on;
- historical operating reports (*e.g.,* error and exception reports) to determine whether the provider's performance aligns with the TCBO's risk appetite; and
- testimonials from other financial institutions on conversion experience.

Negotiating favorable contract terms is an important aspect of the conversion process, though the Board recognizes that TCBOs may have limited leverage in such negotiations. Contractual considerations may include:

- whether the contract provides a reasonable and transparent pricing structure. The TCBO may seek to negotiate provisions about the costs of upgrades to enable compliance with evolving regulatory requirements; variable costs impacted by the number of accounts the TCBO maintains on the core system, the TCBO's asset size, or its transaction volume; whether billing statements are required to clearly explain each service that is being charged; and how long the ''back billing'' window is for the core provider

to issue retroactive charges for items missing from prior invoices.

- whether the terms of the contract are reasonable and transparent, including initial term length and automatic renewal conditions.
- whether the third party is subject to SLAs with measurable performance standards that reflect the TCBO's individual needs and risk profile, along with provisions that enable the TCBO to monitor and enforce the SLAs.
- liability provisions that reflect the criticality of core banking services, with appropriate indemnification for security breaches, intellectual property claims against the TCBO, and data protection violations.
- flexibility to terminate the relationship, taking into account the conditions under which termination is allowed and any fees the TCBO will incur.

2. Information Technology (IT) Infrastructure Providers

Many TCBOs use IT infrastructure providers to deliver foundational services for their technology environment, including cloud hosting, software applications, and physical infrastructure.

Overarching Risk Management Considerations

Disruption to an IT infrastructure provider's networks and systems could significantly impact the TCBO's internal operations and the delivery of products and services to customers. It could also expose sensitive customer data. Consequently, operational and financial resilience and information security are all important risk factors to consider when engaging with IT infrastructure providers; and a TCBO may benefit from considering the risk management strategies for these areas discussed in Section IV.B.

Transitioning to a Cloud-Based Infrastructure Provider

Depending on its business model, a TCBO may realize significant benefits from migrating to a cloud-based IT infrastructure, including reduced capital expenditure, improved scalability, and access to advanced computing resources and security capabilities. However, cloud migration may also involve significant operational complexity, depending on the implementation model a TCBO chooses.

TCBO cloud migrations can vary significantly. For example, a minimalist migration could be limited to applications that have already been optimized for the cloud, such as office productivity suite applications. A TCBO may also choose to migrate individual applications, such as loan processing systems and customer relationship systems. A maximalist migration would include a TCBO's entire IT infrastructure, including all its information systems. Each decision carries different tradeoffs with respect to complexity, cost, and expertise. There can also be variation in how specific applications are migrated. For example, a TCBO may choose to simply replicate its existing loan management system in the cloud; alternatively, a TCBO could choose to modify the application to optimize it for the cloud.

Such choices can impact the operational complexity of a TCBO's migration and have implications related to the degree of IT expertise that it will need to oversee its cloud-based systems. As a general matter, many cloud service providers (CSPs) have resources to help TCBOs understand the provider's offerings and assess what implementation model best fits the TCBO's individual needs. A TCBO may benefit from discussing with the CSP:

- the level of in-house expertise the TCBO will need for a successful migration;
- the categories of data to be migrated and any compromises to data accuracy and integrity that might arise; and
- how operational disruptions during the transition can be minimized, and how the TCBO will be notified of material incidents, consistent with applicable rules and regulations, when information systems are successfully migrated.

As part of its planning for a cloud migration, a TCBO may consider various operational aspects of the transition, including how the TCBO will dispose of physical equipment and transfer or cancel software licenses.

A TCBO may benefit from becoming more familiar with the types of audits and periodic assessments its infrastructure provider conducts, and how this information captures security and performance metrics. In general, infrastructure providers will capture their reporting through customizable dashboard interfaces, which the TCBO can rely on for ongoing monitoring activities. For example, many infrastructure providers allow customers to view how the contracted services are complying with standards and customer-driven compliance rules.

3. Cybersecurity Providers

TCBOs often rely on cybersecurity vendors to help protect their information systems, networks, and data. Among other things, these third parties offer products and services that can bolster defenses against attacks, detect malicious activity, and help TCBOs respond to and recover from cybersecurity incidents. In many cases, an IT infrastructure provider may provide cybersecurity services in connection with its products and services.

Overarching Risk Management Considerations

Cybersecurity has increasingly become an operational imperative for banking organizations. To the extent a TCBO depends on a third party for its cybersecurity, that third party's operational resilience becomes a key risk management consideration.[10] A vendor's information and systems security are also important considerations, given that cybersecurity providers often have access to a TCBO's sensitive information, including customer data. The discussion on how to manage these issues in Section IV.B is generally relevant to cybersecurity vendors.

Specific Risk Management Considerations

An ineffective cybersecurity vendor can make a TCBO vulnerable to cyber incidents, which can lead to financial losses. For example, cyber incidents can cause operational disruptions to banking portals, ATMs, or other services, which, in turn, can drive customers to competitor banking organizations or cause loss of confidential customer information, leading to regulatory fines and customer lawsuits.

To assess the effectiveness of a cybersecurity vendor's product or service, either as part of due diligence or ongoing monitoring, a TCBO may consider:

- reviewing independent assessment reports (*e.g.,* SOC 2 reports and ISO reports);
- consulting with peer banking organizations;
- reading publicly available reviews of the third party's product and service capabilities; and
- reviewing system performance reports and analyzing error rates (*e.g.,* false positives or negatives), mean time to detect threats, and testing the accuracy of threat detection through simulated exercises.

[10] For example, a past significant failure by an infrastructure and cybersecurity provider in delivering global internet traffic to its customers caused widespread customer website outages.

If a TCBO has specific standards or requirements [11] that it needs a cybersecurity provider to meet (*e.g.,* computer-security incident notification requirements, periodic reviews or audits, state privacy laws, data processing and retention timelines, encryption requirements, system availability standards, and multi-factor authentication requirements), it may benefit from incorporating those standards into the governing contract as SLAs. A TCBO may also benefit from obtaining contractual rights to adjust threat detection sensitivity to reflect the TCBO's risk tolerance and review output reports on a periodic basis to ensure that the vendor is complying with agreements.

4. Payment Processing and Digital Banking Providers

Payment processing and digital banking providers deliver transaction and account management services including wire transfers, ACH origination, peer-to-peer payments, bill pay, mobile/online banking portals, treasury management platforms, commercial or retail digital banking services (customer facing mobile and digital applications), and customer service/call center operations. This may also include third-party payment processors engaged by TCBOs, rather than by a TCBO's customer.

Overarching Risk Management Considerations

A payment processing and digital banking provider's operational resilience is a significant risk consideration, since disruptions can prevent customers from accessing accounts and making payments. The strategies for managing these risks discussed in Section IV.B are generally applicable to payment processing and digital banking providers. In addition, a TCBO may consider developing tested backup processing methods, such as switching payments to another processing rail or manually processing time-sensitive transactions.

Payment processing and digital banking providers often support a TCBO's adherence to payment network rules. To help manage these risks, a TCBO may benefit from consulting the compliance discussion in Section IV.B. In addition, a TCBO may consider assessing whether a payment processor is in good standing with the relevant payment network. Payment networks typically require payment processors to conduct audits or file attestations to remain in good standing. Examples include annual NACHA audits and FedLine Solutions Security self-assessments. These reports can help the TCBO assess the third party's ongoing ability to process transactions and secure data consistent with network rules, and maintain the bank's access to critical payments infrastructure.

Finally, the provider's information security can be another important focus area, since payment processing and digital banking providers typically maintain customer credentials and transaction data, and security breaches affecting the vendor could expose sensitive customer data. The discussion of information and systems security in section IV.B is generally relevant to managing these risks.

Specific Risk Management Considerations

Different payment channels require different data processing capabilities. For example, instant payment channels may require higher frequency data exchanges than channels that rely on batch processing. As part of due diligence, a TCBO may benefit from verifying that its payment processor has the data processing capabilities for the payment channels it wants to offer customers, as well as the ability to effectively feed information into compliance and fraud detection systems. To do this, a TCBO can consider requesting product demonstrations that reflect its individual specifications and business needs.

As part of routine monitoring of payment processing and digital banking providers, a TCBO may consider:

- the quality and accuracy of system-generated alerts to identify any posting or reconciliation issues between payment processing systems and core systems;
- analyzing relevant customer complaints to identify recurring or emerging issues; and
- reviewing failed transactions or discrepancies to verify whether the systems accurately flagged issues.

5. Loan Management System Providers

Loan management system providers support some or all elements of the lending lifecycle from origination through payoff. They generally provide loan origination platforms, loan servicing systems, document management solutions, and lending compliance tools.

Overarching Risk Management Considerations

Loan management system failures can halt new loan originations, prevent loan servicing activities, and disrupt loan payment processing. Given that loans typically constitute the largest asset class for TCBOs, such problems can quickly become a material threat to a TCBO's business. Thus, a loan management system provider's operational resilience is an important focus area, and TCBOs may benefit from consulting the operational resilience considerations discussed in Section IV.B. In addition, a TCBO may consider whether it can temporarily substitute manual processes for the third party's services in the event of sustained disruption.

Loan management systems also contain extensive personal and financial information. Security breaches affecting loan systems can expose sensitive borrower information with significant potential for identity theft and fraud. The discussion of systems and information security in Section IV.B may be useful in managing these risks.

Specific Risk Management Considerations

Loan management systems are designed to originate, process, and/or service loans based on the TCBO's established credit risk management practices and underwriting standards. Some loan management systems may use automated credit decisioning or risk scoring approaches. During due diligence, a TCBO may consider the third party's ability to consistently apply the TCBO's credit policies as part of this automation. For example, a TCBO may have specific requirements for certain loan types (*e.g.,* oil and gas loans require specific structures, covenants, or collateral that must be configured into the system). A TCBO can verify these requirements are being met through implementation testing. In addition, a TCBO can consider whether the third party can support the TCBO's efforts to maintain compliance with applicable lending laws, and scale with portfolio growth.

Unlike payment processing where errors are often identified quickly, loan origination or processing errors may remain undetected for extended periods, allowing errors to accumulate, create loan origination backlogs, delay loan closings, and prevent customers from accessing credit during the disruption period. Examples include automated credit scorecards miscalculating debt ratios due to incomplete data, incorrect past-due date calculations that generate

[11] *See e.g.* Computer-Security Incident Notification, 12 CFR 225.303 (bank service provider notification).

erroneous late fees, or incorrect interest compounding frequencies. To assess the risk that a provider's systems are prone to such errors, a TCBO may consider reviewing independent assessments (such as independent audits or SOC reports) for controls effectiveness, past regulatory violations, or publicly available complaints databases such as Consumer Financial Protection Bureau (CFPB) Consumer Complaint Database.

A TCBO may benefit from sampling loan files to verify that they are booked accurately, contain the required disclosures, are delivered timely, and are properly documented. A TCBO remains responsible for accurate loan processing and disclosures, and may consider contractual provisions requiring the third party to indemnify the bank for losses caused by third-party errors, maintain appropriate insurance coverage, and provide the TCBO access to system documentation or the right to audit third-party processes.

6. Card Issuing and Processing Providers

Card issuing and processing third parties provide a range of services for debit card, credit card, and ATM card programs, including card production, network integration, transaction authorization, settlement processing, dispute resolution, fraud monitoring, and bank-identification-number (BIN) sponsorship arrangements. BIN sponsorship is necessary when the TCBO does not have direct membership in a card network (*e.g.,* Visa or Mastercard). The BIN sponsoring bank acts as issuer of the cards, while the TCBO maintains the customer relationship.

Overarching Risk Management Considerations

Operational resilience is a significant consideration, since system failures, network disruptions, or processing errors can prevent customers from accessing their funds, completing purchases, or withdrawing cash. Financial resilience can become particularly important when a TCBO relies on a BIN sponsor; if the BIN sponsor becomes insolvent, the TCBO could lose network access, forcing rushed program termination and card reissuance. For co-branded card programs with merchant partners, partner insolvency may leave the institution liable for unpaid rewards obligations. System and information security is also a material overarching risk management consideration. Card programs involve continuous transmission of sensitive cardholder data across multiple parties and networks, resulting in multiple points of entry for security breaches. Finally, the provider's adherence to network rules is a relevant consideration.

In addition to the strategies for addressing these risks discussed in Section IV.B, a TCBO may review a processor's network compliance certification and monitor network bulletins for security events. Further, card networks generally require processors to maintain PCI DSS attestations and reports of compliance, where applicable. These attestations and accompanying reports can assist TCBOs with evaluating the third party's security risk management practices in alignment with risk appetite.

Specific Risk Management Considerations

In cases where a TCBO is transitioning card service providers, the TCBO may consider the following to minimize service disruptions:

- keeping the old processor active while bringing the new one online to avoid customer card outages;
- developing communication strategies to inform customers of card replacement timing, activation procedures, and payment arrangements that may require updating;
- validating the accuracy of card holder data (*e.g.,* active/inactive cards, fraud blocks, or temporary holds) to ensure accurate reissuing, if necessary; and
- coordinating with outgoing and incoming BIN sponsors to migrate card holder data, test network access, and re-issue cards (if applicable).

As part of ongoing monitoring, a TCBO may benefit from reviewing customer complaints and system-generated alerts related to card authorization failures, fraud incidents, or dispute resolution to assist the TCBO in identifying recurring issues or service quality concerns. Furthermore, a TCBO may monitor card processing reports to ensure third parties and processors are not issuing outside of agreement.

7. BSA/AML and Financial Crime Platform Providers

BSA/AML and financial crime platform providers deliver transaction monitoring, sanctions screening, currency transaction reporting (CTR), suspicious activity reporting (SAR), Customer Due Diligence (CDD), and Customer Identification Program (CIP) services.

Overarching Risk Management Considerations

The principal risk to a TCBO from BSA/AML third parties is the impact on the TCBO's ability to comply with banking regulations. System failures, configuration errors, or inadequate transaction coverage can result in the TCBO facilitating money laundering or terrorist financing and regulatory violations. While operational resilience of BSA/AML vendors can be important, TCBOs may be able to rely on manual workarounds in the event of interruptions. System and information security is also a key risk consideration, as security breaches affecting BSA/AML platforms could expose sensitive customer information and investigation details. A TCBO may benefit from reviewing the risk management strategies on these issues discussed in Section IV.B.

Specific Risk Management Considerations

In deciding on appropriate BSA/AML tools that meets its compliance needs, a TCBO may consider reviewing vendor system documentation to understand detection rules, logic, thresholds, and scenario coverage for alignment with its risk profile and applicable regulatory guidance (*e.g.,* FinCEN advisories and sanctions lists). A TCBO may benefit from considering the extent to which its BSA/AML provider aligns with the TCBO's risks and business profile. For most TCBOs, basic BSA/AML tools will be sufficient. Where, however, a TCBO's clients present higher risk (*e.g.,* marijuana-related businesses), tools with more advanced capabilities may be appropriate.

As part of ongoing monitoring, a TCBO may consider analyzing scenarios that generate excessive false positives or do not generate any useful alerts. Increasing false positive rates may indicate system tuning is needed, while decreasing alert volumes may indicate system issues or that tuning is too lenient. Additionally, a TCBO may consider verifying that the third party delivers timely sanctions list updates and regulatory changes.

Contract negotiation is also important in managing compliance risks associated with BSA/AML and financial crime platform providers. When negotiating contracts, a TCBO may consider:

- clarifying the third party's responsibilities for maintaining system compliance with BSA/AML regulations, FinCEN requirements, and applicable examination guidance. This could include sanctions list updates and rule changes within defined timeframes;
- the TCBO's rights to tune alert thresholds, modify transaction monitoring scenarios, and adjust risk scoring parameters, including any associated costs and timeframes; and

• the TCBO's ownership of customer data, alert histories, investigation documentation, and SAR filings, with rights to access and extract data throughout and beyond the contract term.

8. Fraud Prevention and Detection Providers

Fraud prevention and detection providers offer real-time fraud monitoring, device fingerprinting, behavioral analytics, identity verification tools, and authentication services across banking channels. A TCBO may receive these services embedded in another provider's solution (*e.g.,* the TCBO uses fraud prevention and detection tools provided through its payment and card processor), or establish separate relationships to address shortcomings in fraud prevention or detection for specific delivery channels, products, or transaction stages.

Overarching Risk Management Considerations

Fraud prevention tools typically operate in real time to prevent fraudulent transactions before they occur. Operational resilience is important because system failures can immediately affect the customer experience—either by blocking legitimate transactions or allowing fraudulent transactions to proceed, potentially leading to operational losses at the TCBO. System and information security is important, as these tools may include access to sensitive customer information such as biometrics and authentication credentials. Failures to implement appropriate fraud risk management systems could result in the TCBO being in violation of network rules. The discussion of these issues in Section IV.B may be helpful as a TCBO considers how to manage these risks.

Specific Risk Management Considerations

A fraud detection tool's effectiveness can depend on how thoroughly and promptly it can take advantage of fraud intelligence data. During due diligence, a TCBO may consider the third party's ability to integrate with multiple data sources, including other third-party systems and threat intelligence feeds (such as dark web monitoring and shared fraud databases), and apply them to identity verification and transaction authorization controls.

Many of the risk management strategies that apply to BSA/AML providers are equally relevant to fraud prevention and detection providers. As with BSA/AML providers, ongoing monitoring of fraud prevention and detection providers can include analyzing trends in fraud alerts, customer complaints, and scenarios that generate excessive false positives, as increasing false positive rates may indicate system tuning is needed, while decreasing alert volumes may indicate system issues or tuning that is too lenient. A TCBO may also consider the extent to which the provider can calibrate its model based on the TCBO's direction in keeping with the TCBO's risk appetite.

In addition, when the service provider plays a role in customer communication and investigating disputes, a TCBO may consider tracking investigation and resolution timelines to ensure compliance with contractual commitments and regulatory requirements.

By order of the Board of Governors of the Federal Reserve System.

Benjamin W. McDonough,

Secretary of the Board.

[FR Doc. 2026–18852 Filed 9–14–26; 8:45 am]

BILLING CODE 6201–01–P

FEDERAL RESERVE SYSTEM

Formations of, Acquisitions by, and Mergers of Bank Holding Companies

The companies listed in this notice have applied to the Board for approval, pursuant to the Bank Holding Company Act of 1956 (12 U.S.C. 1841 *et seq.*) (BHC Act), Regulation Y (12 CFR part 225), and all other applicable statutes and regulations to become a bank holding company and/or to acquire the assets or the ownership of, control of, or the power to vote shares of a bank or bank holding company and all of the banks and nonbanking companies owned by the bank holding company, including the companies listed below.

The public portions of the applications listed below, as well as other related filings required by the Board, if any, are available for immediate inspection at the Federal Reserve Bank(s) indicated below and at the offices of the Board of Governors. This information may also be obtained on an expedited basis, upon request, by contacting the appropriate Federal Reserve Bank and from the Board's Freedom of Information Office at *https://www.federalreserve.gov/foia/request.htm.* Interested persons may express their views in writing on the standards enumerated in the BHC Act (12 U.S.C. 1842(c)).

Comments received are subject to public disclosure. In general, comments received will be made available without change and will not be modified to remove personal or business information including confidential, contact, or other identifying information. Comments should not include any information such as confidential information that would not be appropriate for public disclosure.

Comments regarding each of these applications must be received at the Reserve Bank indicated or the offices of the Board of Governors, Benjamin W. McDonough, Secretary of the Board, 20th Street and Constitution Avenue NW, Washington, DC 20551–0001, not later than October 15, 2026.

A. Federal Reserve Bank of Minneapolis (Mark Nagle, Assistant Vice President) 90 Hennepin Avenue, Minneapolis, Minnesota 55480–0291. Comments can also be sent electronically to *MA@mpls.frb.org:*

1. *Profinium Financial Holdings, Inc., Fairmont, Minnesota;* to acquire F&M Community Bank, N.A., Preston, Minnesota.

Board of Governors of the Federal Reserve System.

Benjamin W. McDonough,

Secretary of the Board.

[FR Doc. 2026–18861 Filed 9–14–26; 8:45 am]

BILLING CODE P

FEDERAL TRADE COMMISSION

Civil Penalty Inflation Adjustments

AGENCY: Federal Trade Commission.

ACTION: Notice.

SUMMARY: In accordance with guidance from the Office of Management and Budget (''OMB''), the Federal Trade Commission (''FTC'')'s civil penalty amounts will remain unchanged during 2026. The FTC will continue to apply the 2025 civil penalty levels.

DATES: Effective September 15, 2026.

FOR FURTHER INFORMATION CONTACT: Marie Choi, Attorney (202–326–3368), Office of the General Counsel, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

SUPPLEMENTARY INFORMATION: The Federal Civil Penalties Inflation Adjustment Act Improvements Act (''FCPIAA'') of 2015 directs Federal agencies to annually adjust each civil monetary penalty under their jurisdiction for inflation pursuant to a cost-of-living adjustment.[1] The cost-of-living adjustment is based on the percent change between the U.S.

[1] Public Law 114–74, 701, 129 Stat. 599 (2015). The Act amends the Federal Civil Penalties Inflation Adjustment Act, Public Law 101–410, 104 Stat. 890 (codified at 28 U.S.C. 2461 note).