Third-Party Risk Management, Compliance Standards

Cite:
FRB, OCC, FDIC; Proposed Inter-Agency Guidance

Recommended Distribution:
Risk Management, Corporate Development, Corporate Planning, Policy, Legal, Government Relations

Website:
https://www.federalregister.gov/documents/2021/07/19/2021-15308/proposed-interagency-guidance-on-third-party-relationships-risk-management

Impact Assessment

- Dramatically expanding the regulatory perimeter, new indirect risk-management/compliance standards could reach not only to all tech vendors, but also to fintech partnerships, bigtech platforms, affiliates/subs, and nonbank parent companies.
- This will enhance safety and soundness and reduce contagion risk, but also create new obstacles to innovative product offerings, digitalization, and corporate expansion.
- "Rent-a-bank" relationships and banks that ride on tech-platform companies would face additional challenges consummating relationships, ensuring ongoing compliance.
- Banks are allowed to negotiate with third parties to gain the market strength likely needed to win concessions securing bank compliance (e.g., from cloud-service providers). However, such cooperation could lead to collusion assertions by third parties or newly-vigilant antitrust enforcers.
- Banks may now gain new insight into consumer-reporting agencies as these would be considered third-party vendors subject to extensive due-diligence, monitoring, risk-management, consumer-compliance, and contractual commitments.
- Although issued as guidance, violations of new standards could result in enforcement actions specified in the proposal.
- Although clearly intended as sweeping, the standards nonetheless are not always consistent about covered third-parties. The overall list of covered entities and relationships is broad, but various new duties appear in some cases applicable only to more traditional relationships.

Overview

The banking agencies have proposed sweeping standards that would hold all of the banking organizations they govern responsible for the safety and soundness, consumer compliance, and perhaps even diversity of a wide range of third-party business arrangements that now expressly bring in affiliates, subsidiaries, and parent holding companies along with the full scope of outsourced product and service relationships, marketing partnerships, joint offerings, and even use of a third-party mobile phone platform. Much of what would be required of banks may be feasible within contractual relationships, but the guidance would apply even when there is no exchange between the bank and a third party. When these relationships are indirect – e.g., distribution of services via third parties with whom the bank has no relationship – it may be challenging for banks to assure themselves of suitable risk mitigation and compliance, structurally changing many aspects of how a bank offers services, uses technology vendors, interfaces with fintechs and bigtechs, underwrites credit, and engages in otherwise-impermissible activities through a third party or by affiliation with a parent company. Significant enforcement penalties would be possible for failures to comply with the guidance's extensive risk-management, governance, and compliance requirements.

Impact

If finalized, this guidance would replace each agency's exiting vendor risk-management requirements, each of which differs in substance and application. In doing so, this would limit regulatory arbitrage as well as raise standards uniformly across the sector addressing not only a wider range of activities than most had previously contemplated, but also emerging technologies and activities that might otherwise pose risk to banks, consumers, the financial system, or even the economy.

In the past, the banking agencies principally focused third-party risk-management efforts on vendors of critical technology services.[1] The general thrust of these standards was to address information security in hopes of ensuring that bank and bank-customer information was secure even if processed by a third party. However, in 2020, the OCC issued frequently-asked questions (FAQs) that broadened the agency's reach to alternative-data, cloud-services, payment providers, consultants, data aggregators, and any entity with which the bank has a contractual or other service relationship.[2] The proposed guidance is in many places phrased more broadly than the FAQs, encompassing for example also the consumer-reporting firms now exempt from the reach of indirect bank-regulatory requirements and entities with which a bank has a "relationship" even if not contractual or otherwise subject to direct compensation.

The OCC also set policy related to third-party lending arrangements in its controversial 2020 true-lender rule,[3] which included language requiring national banks to ensure effective risk-management and consumer-protection compliance

[1] See *Client Reports* in the **VENDOR** series.

[2] See **VENDOR8**, *Financial Services Management*, March 18, 2020.

[3] See **PREEMPT35**, *Financial Services Management*, November 2, 2020.

when working with fintechs or others in a relationship sometimes called "rent-a-bank." That rule has since been struck down by Congress and President Biden, but the FAQs establish a national bank's duties when a fintech or other entity has a relationship issuing loans or otherwise offering services in partnership with the bank.

This is less clear in the guidance, which establishes a clear bank duty, but could be read in some places as confining it only to arrangements with entities or individuals providing services that could expose the bank to significant operational risk. Conversely, the proposed guidance clearly exempts "customers," perhaps differentiating it from the FAQs by virtue of considering a person who buys loans initially made by the bank to be its "customers." The agencies seek comment on whether to incorporate all of the FAQs into their final standards, which might clarify the reach of each statement and reduce any remaining opportunity for regulatory arbitrage.

However, even if the final guidance is in some ways more limited than the OCC's approach, it would have significant strategic impact. It starts with its formal statement that banks are responsible for the safety and soundness and consumer compliance of any third party (now broadly defined in most places), continuing in detail often to assign still more specific duties, especially with regard to corporate governance.

This expanded scope is particularly germane to the Fed's liberalized approach to determining when direct or indirect "control" exists over a third-party, triggering requirements to form a bank holding company. Although the thrust of this rule addresses direct investment, it also captures "business relationships" that could create indirect control. This could trigger the guidance's risk-management requirements, thus creating strategic challenges as well as enhanced risk mitigation regardless of the extent to which the business relationship is deemed permissible under the Bank Holding Company Act.

Indeed, the guidance would go farther and address not only entities brought within this new, broad definition of third parties, but also entities – affiliates and parent holding companies – previously considered "second" parties or even the equivalent of an insured depository. The scope of this expansive coverage could be very far-reaching. It would for example cover the parent holding companies of industrial banks or the other entities addressed to some extent in controversial 2020 FDIC standards for non-traditional parent companies,[4] expanding the FDIC's reach through the insured depository to key aspects (e.g., information security, consumer protection) beyond the scope of its prior focus on source-of-strength capacity. Reaching to parent companies and affiliates could also lead to more de facto combined safety-and-soundness standards based on home-country parent companies and the branches and agencies affiliated with insured depositories controlled by foreign banking organizations.[5]

[4] See **ILC15**, *Financial Services Management*, December 21, 2020.

[5] See **SIFI34**, *Financial Services Management*, October 23, 2019.

The strategic impact of these risk-management standards will depend on an observer's perspective. On the one hand, they could sharply limit "rent-a-bank" arrangements at least with regard to those aimed at skirting consumer-protection standards (controversial state usury-ceiling exemptions are not directly addressed in this guidance). This would generally enhance consumer protection as well as protect banks from unanticipated litigation and the safety-and-soundness risks related to poor underwriting that could lead to bank recourse even in the absence of contractual commitments to provide it. Conversely, these standards might limit credit availability and product innovation to the extent regulatory risk-management requirements are inconsistent with sound activities.

These standards could also bring critical payment and cloud-service infrastructure closer to the regulatory perimeter. This would address a range of concerns from FSOC, Congress,[6] and many banks related to the concentrated number of cloud-service providers increasingly proving a vital form of core financial infrastructure. The same is true of the risks posed by concentrated payment-service providers with direct access to bank transaction accounts or key interfaces with bank payment processing as well as the increasing dependence banks have on tech-platform companies handling payments or other product offerings.

The proposal is at pains to make clear that supervisory expectations related to third-party relationships will be tailored to the size and complexity of a bank and the importance of the relationship to a bank. Although it would also permit use of companies, utilities, or other entities that evaluate third-party risk, the guidance would go farther, allowing banks to collaborate in fulfilling their risk-management obligations and even jointly negotiating contracts with third parties. This is clearly aimed at small banks, but even then might raise concerns about undue collusion or other anti-competitive effects. The guidance does admonish companies to be mindful of antitrust considerations, referencing current FTC and DOJ statements. However, the current antitrust context is considerably more challenging, with the FTC under new leadership and the overall antitrust construct now under an executive order detailing a far tougher approach to curbing anti-competitive activity.[7] As a result, collaboration along lines authorized by the guidance could pose additional risks if not carefully considered.

In addition to holding a bank responsible for the safety and soundness and consumer compliance of third parties, the guidance also suggests broader responsibilities, thus going beyond the 2020 OCC FAQs. Details in the guidance clearly assign additional responsibilities for broader regulatory compliance with the full scope of domestic and international law to which the bank is subject. Banks are also to consider the extent to which the third party's employment practices are consistent with its own, considering also policies for diversity and inclusion. Where banks have power over contractors, this might enhance good practice; where it does not, this potential additional due-diligence requirement could be challenging.

What's Next

This proposal was issued on July 13; comments are due September 17.

[6] See **FEDERALRESERVE53**, *Financial Services Management*, February 11, 2020.

[7] See *Client Report* **MERGER6**, July 9, 2021.

As discussed below, the guidance makes clear that banks could be subject to enforcement and related penalties if they fail to comply with its sweeping requirements. However, the banking agencies have recently said that they will not use guidance for any standards that could result in enforcement in a fashion different than that of the rules to which a guidance pertains. If commenters persuade the agencies that this policy applies to the third-party guidance, a regulatory proposal would be required to implement it.

Analysis

Although much in the proposed guidance tracks the OCC's 2020 FAQs, the agencies nonetheless say that, unlike all their other vendor standards, it is not incorporated in this proposal. Instead, it is treated as a supplement to the proposed guidance, with comment sought on whether it should be more directly incorporated in final guidance.

A. Scope

1. Relationships

A third-party relationship would be any business arrangement between a banking organization and another entity, by contract or otherwise. An exchange of money is not necessary to create such a relationship. Covered relationships include those for or with:

- technology services;
- credit scoring;
- mobile-phone services;
- providing banking services through the third party's platform;
- innovative product offerings;
- fraud detection;
- AML compliance;
- customer service;
- merchant payment processing;
- networking arrangements;
- arrangements with other banks;
- other outsourced products and services;
- independent consultants;
- affiliates, subsidiaries, joint ventures, and any other business arrangement where the bank has an ongoing relationship with a third party and has responsibility for associated records; and
- the parent company.

2. Collaboration

As noted above, banks could share risk-management information, perform joint due diligence, and even negotiate contracts as groups or presumably even as an industry.

3. Sub-Contractors

Due-diligence standards would extend to sub-contractors, with the guidance laying out how banks are to address this risk when entering into third-party relationships, monitor them, and track risk.

B. Information Security

The standards prescribe an array of due-diligence, monitoring, and risk-management controls to enhance information security. These build on existing standards,[8] but address many issues – e.g., data privacy – that have taken on new significance.

C. Governance

The new standards state that it is the policy of the FRB, OCC, and FDIC that banks have responsibility for risks and compliance related to third-party relationships regardless of any outsourcing or hold-harmless provisions, and directors are responsible for ensuring this. Use of external services (e.g., utilities, consortia) does not abrogate the board's responsibility to ensure effective bank risk management and compliance, with the board also told to ensure periodic independent audits. The guidance also stipulates many other aspects of board responsibility (e.g., contract review) that may impinge on day-to-day management, often duplicating tasks also expressly assigned to senior management.

D. Vendor Life Cycle

In a new section, the guidance also details the life cycle of critical outsourced business and third-party relationships, stipulating that through-the-cycle risk management is required to ensure at all times that safety and soundness and compliance are maintained in any relationship "critical" to the bank (i.e., essential for core services, not substitutable, or with major operational impact). It is not clear if the very detailed life-cycle requirements thus apply only to operationally-significant third-party relationships or to all the others specified in the guidance.

E. Supervision

The guidance also provides extensive detail on how examiners will assess bank performance. It makes clear that any lapses would be serious and potentially subject the bank to enforcement action (see above), also noting that performance of third-party standards may be judged in the M rating for a bank's CAMELS score. The standards also reiterate the ability bank examiners have to review the third party directly, looking at its ability to perform its contractual obligations to the bank and comply with applicable law and rule.

F. Request for Comment

In addition to seeking comments on how the 2020 FAQs should be reflected in final inter-agency guidance, comment is solicited on:

- the extent to which the standards are properly tailored to banks and activities;
- the scope of covered relationships;
- the need for changes or additional standards related to foreign providers;

[8] See *Client Reports* in the **INFOSEC** series.

- ways to better address challenges negotiating with third parties;
- ways to encourage industry collaboration without anti-competitive effect;
- the benefits of revising the guidance related to sub-contractors by clearer, "fourth-party," requirements and if critical arrangements involving sub-contractors require additional scrutiny;
- the need for additional information-security standards; and
- how best to treat the OCC's 2020 FAQs.

Federal Financial Analytics, Inc.
2101 L Street, N.W., Suite 300, Washington, D.C. 20037
Phone: (202) 589-0880
E-mail: info@fedfin.com Website: www.fedfin.com