Third-Party Relationship Requirements

Cite

OCC; Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29

Recommended Distribution:

Fintech, Risk Management, Compliance, Policy, Legal, Government Relations

Websites:

https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-10.html

Impact Assessment

- National banks now fall under additional restrictions in fintech relationships, using alternative data, relying on payment processors, and deploying cloud-service providers. Innovation may slow, but risk will be better mitigated.
- Restrictions may also slow fintech access to bank-customer data, enhancing competitiveness for national banks able to retain consumer loyalty.
- National banks may continue to rely principally on traditional credit scores due to new restrictions on alternative data.
- New corporate-governance standards may be necessary.

Overview

The OCC has decided to update and in several respects substantively revise 2013 standards on third-party vendors with frequently-asked questions (FAQs) that lay out new official views in an arena of growing importance due to "rent-a-bank" arrangements, cloud computing, the growing use of data aggregators, and other fintech developments. The new FAQs also rescind a 2017 FAQ statement dealing with some of these questions, although all of it is retained largely unchanged.[1] As in its prior statements, the OCC here emphasizes that using a vendor or third party to perform a function does not absolve a national bank of its responsibility to ensure effective risk controls, with more due diligence, monitoring, and control needed as the importance of a third-party relationship increases. This obligation is not absolved by a bank's lack of negotiating power – a common community-bank concern – but new procedures are detailed to make it possible for banks still to do business with third parties in such cases. Banks may also do business with data

[1] See *Client Report* **VENDOR7**, September 12, 2017.

aggregators, but must have risk-mitigation protocols of increasing strength to safeguard consumer information and ensure security based on the business relationship. If only screen-scraping is involved, the bank need not block access as long as it is persuaded that the scraper is a legitimate, sound organization. Although the agencies have generally encouraged banks to use alternative credit-risk indicators,[2] new model-related risk protocols impose additional constraints on national banks that choose to do so. No such restrictions apply to existing consumer reporting agencies, perhaps encouraging ongoing reliance on established credit scores.

Impact

Bank-regulatory interest in third-party vendors waxes and wanes with the sins these vendors are seen to commit. The regulatory framework was codified first with respect to the OCC's ability to charge examination fees in this case,[3] with other actions including inter-agency guidance,[4] FFIEC standards,[5] and FDIC requirements.[6] Most recently, the Treasury Department under President Obama recommended that the banking agencies consider their service-company authority to govern online-marketplace lenders working with insured depositories;[7] the OCC acted in 2017 to tighten its standards for these lenders. The FDIC proposed similar guidance in 2016,[8] but never finalized it.

However, rapid tech-finance developments and growing challenges outside the online-marketplace lending arena have created uncertainties and risk the OCC addresses in these new FAQs. For example, the Capital One cyber-security breach raised many questions about a bank's responsibility related to a cloud-service provider.[9] The FAQs make it very clear that national banks are responsible for ensuring not only system integrity and continuity, but also for configurations associated with cloud computing even if these are stipulated by the provider. National banks are also not absolved of responsibility if the cloud-service provider is unwilling or unable to provide the information banks require to ensure that they comply with these FAQs and other risk-management standards. This framework may put Amazon and other providers under greater pressure to increase transparency, but if providers remain reluctant, banks will either take on additional risk or slow innovation at cost to operational efficiency and service.

Data aggregation is also a heightened OCC concern. The new FAQs go beyond prior guidance to stipulate that national banks must control data flows to screen-scrapers even if they have no business relationship with the aggregator if

2 See **FCRA29**, *Financial Services Management*, December 11, 2019.
3 See **VENDOR4**, *Financial Services Management*, May 25, 2001.
4 See **VENDOR5**, *Financial Services Management*, May 2, 2003.
5 See **VENDOR2**, *Financial Services Management*, December 11, 2000.
6 See **VENDOR6**, *Financial Services Management*, June 18, 2008.
7 See **FINTECH2**, *Financial Services Management*, May 24, 2016.
8 See **LENDING8**, *Financial Services Management*, August 16, 2016.
9 See *Client Report* **CYBER28**, August 15, 2019.

due diligence suggests system-integrity or-privacy risk. Banks are also told to identify scraping, track the firm doing it, and institute controls as or if needed. This gives national banks a clear legal rationale to refute assertions that consumer financial data are solely the property of the consumer and thus must be released to a third party if that entity can demonstrate that a consumer has asked it to do so. The OCC's approach is in line with CFPB guidance in this arena,[10] which rolled back proposed requirements that banks share data whenever requested to do so.[11]

The new FAQs are also cautious when it comes to alternative-data use despite the broad authorization recently provided for its use. This will reinforce national-bank reluctance to move to alternative credit-underwriting systems, perhaps diminishing innovation and financial inclusion but also enhancing risk mitigation in areas such as fair lending. Alternative-data vendors may demand like-kind model validation for traditional consumer reporting agencies.

What's Next

The OCC issued these FAQs on March 5. Those opposed to aspects of the new requirements may dispute them on grounds that they establish *de facto* regulatory requirements that should have been advanced only with prior public notice and comment.

Analysis

Key issues addressed in the FAQs include:

- Covered Relationships: As before, these are any business arrangement between the bank and another entity (e.g., vendors, consultants, networks, merchant-payment processors, affiliate/subsidiary services, joint ventures). Relationships may arise due to contracts, referral agreements, cross-marketing, and any other type of relationship that generally does not involve a customer. When sufficient information is not available on critical-service providers, the board and management must establish risk-mitigating controls, ensure redundancy and that the provider is the best possible despite missing information, retain documentation on efforts to obtain documentation, and ensure contracts are robust.

- Cloud Services: Based on the above definition, the FAQ reiterates that cloud-service providers are covered third-party relationships. The FAQs go on to detail the additional controls banks must have in place for any critical cloud-service arrangement due to its structural differences from traditional IT providers (e.g., clear understanding of features the bank is responsible for configuring).

[10] See **FINTECH14**, *Financial Services Management*, October 24, 2017.

[11] See **FINTECH6**, *Financial Services Management*, November 1, 2016.

However, regardless of these agreements, the OCC states that banks are ultimately responsible. If third parties are used to govern cloud subcontractors, banks must ensure that these entities can effectively perform these duties.

- Data Aggregation: The extent to which a bank has a relationship with a data aggregator depends on the formality of the relationship, but any relationship raises risks that the bank must control even if it receives no benefit from the relationship. Data security is to be a top priority. Further, even in the absence of any relationship, banks still take on risks when sharing customer-permitted information, leading the OCC to mandate an array of safeguards, with the FAQs providing details on different relationships, risks, and required mitigation.

- Negotiating Power: Some vendors or other parties do not allow banks, especially smaller ones, to negotiate terms on standard contracts, do not respond to inquiries about business continuity, and otherwise do not facilitate risk mitigation and due diligence. In such cases, the FAQs instruct banks to take mitigating action based on their own risk assessment. This might involve not doing business with the entity, finding other information sources, or recognizing risks and building their own controls and buffers. Documentation about efforts to obtain more information is also required.

- Alternative Data: When considering alternative data from a third party, banks are to conduct due diligence, ensure safety and soundness, apply models-risk management principles, analyze consumer protection law and rule, and conduct monitoring. Any use of third-party alternative data that is a "substantial deviation" from existing practice should be discussed with the OCC.

- Management Responsibility: These include ensuring that subcontractors to third parties are effectively monitored by the third party following procedures in the FAQs, governing collaborative user groups and maintaining independent risk protocols, determining when compliance certificates or similar documentation suffices, having contingency plans when third parties are start-ups with limited financial capacity, supervising outsourced compliance, managing mobile-delivery systems, managing models risk including by supervising third parties and documenting customization choices.

- Board Responsibilities: These include understanding and approving critical-service contracts in sufficient depth to ensure resilience.