BankOnITUSA®

May 27, 2016

By email: innovation@occ.treas.gov

Office of the Comptroller of the Currency
250 E St., SW
Washington, D.C. 20219

Re: *Supporting Responsible Innovation in the Federal Banking System*

Ladies and Gentlemen:

The following suggestions are submitted as comments in response to the above-referenced OCC release dated March 31, 2016. BankOnIT believes that the suggestions listed here can benefit both the OCC and regulated financial institutions by helping to support the process of selecting well-qualified service providers, including those that are on the cutting edge in providing innovative technology. The comments below apply generally to all technology service providers; but these suggestions become increasingly relevant in light of the proliferating number of companies that are now offering technology to financial institutions. As institutions become more and more reliant on service providers to perform "critical activities" that the institutions cannot effectively provide for themselves, it is appropriate for regulators to continue focusing on the financial institutions' process of selecting service providers. The regulatory agencies can take constructive steps to support institutions in the provider-selection process.

1. **The OCC should enforce the notice requirement in 12 USC 1867(c)(2), as written, to allow the OCC to review more promptly a financial institution's selection of new service providers.**

Both the FDIC and the Federal Reserve continue to require financial institutions to provide a notice within 30 days after a new service provider is hired, in compliance with 12 USC 1867(c)(2). But since the 1980s the OCC has waived this statutory requirement for national banks—apparently for "paperwork reduction" reasons. The OCC's current approach is simply to require a financial institution *to retain in its files* a list of all of the institution's service providers.

When this approach was first adopted, the OCC may have decided it was not taking any action before the next examination anyway, in response to information contained in these notices. In today's environment, by contrast, cyber risks and appropriate information security controls have taken on much greater importance. Compared to the 1980s, the number of potential service providers that an institution could hire has increased exponentially, and institutions have greatly expanded the types of "critical activities" being outsourced. Most of a financial institution's sensitive data is now being hosted or backed up remotely, or at least can be accessed remotely by someone.

As technology continues to change rapidly, each new product or system has potential for introducing new security vulnerabilities. New types of Internet-based security attacks keep appearing. The FFIEC's recent guidance has placed major emphasis on the risks of outsourcing, stressing that a bank must carry out adequate due diligence and proper risk evaluation, and must implement appropriate risk mitigation, as well as continuing to supervise and monitor the provider's activities, as part of the process of utilizing any new "critical activities" provider.

Community financial institutions cannot avoid outsourcing some or all of their important "critical activities." Comptroller of the Currency Thomas Curry recently warned that cybersecurity is possibly an institution's most important risk. Outsourcing can effectively reduce certain risks, but at the same time potentially exposes a financial institution to other risks. The effectiveness of a service provider's security controls can be a crucial element in the institution's ability to manage cybersecurity risks effectively.

Another relevant change has occurred since the 1980s, in the length of the OCC's normal examination cycle for well-managed institutions—now 18 months. Although this longer interval between examinations can be appropriate for some purposes, the OCC still may have a legitimate interest in monitoring certain developments more frequently as they occur—particularly, areas of higher risk or rapid technological change.

Deciding to again enforce the notice requirement of 12 USC 1867(c)(2) would give the OCC the ability to maintain a continuously updated internal database showing each national bank's current service providers. Among other benefits, this information could be useful for correlation. For example, if a problem were discovered at a specific institution that uses a particular provider, the OCC could promptly address that problem at every other financial institution using the same provider—instead of learning as much as 18 months later during a normal examination cycle that other institutions have also started using the same provider.

It is not burdensome for financial institutions regulated by the OCC to comply with the same statutory notice requirement that has applied and has been enforced for decades for institutions subject to regulation by the FDIC or the Federal Reserve as primary Federal regulator.

Probably upwards of 90% of the more than 4,000 financial technology firms operating today are not being regularly examined either as banks or as Technology Service Providers (TSPs). Banking regulators are examining more TSPs than ever before, but regulators are appropriately focusing first on providers that serve a larger numbers of institutions. With finite resources available this approach is logical. Still, many service providers remain unregulated—especially providers that are smaller, or those that primarily work for other companies but also serve several financial institutions. (Providers in both of these categories may be less familiar with regulations and security standards specifically applicable to financial institutions.)

If institutions regulated by the OCC were required to submit a notice within 30 days after hiring a new service provider, this would allow the OCC to take various subsequent actions, if appropriate under the circumstances. As one example, the OCC might request supplemental information from a financial institution that is the first one to give notice that it uses a certain service provider. The OCC could also ask to review a copy of the provider's contract with the institution, if the provider is one with which the OCC was not previously familiar. The OCC in its discretion could also ask to review a copy of the due diligence information that the institution has collected on this unknown provider. Going further, in some cases the OCC might even ask to review a copy of the institution's board minutes showing a discussion of the risks and benefits of entering into a contract with that previously unknown service provider.

A decision by the OCC to make use of this already-existing tool—the "new service provider" notice requirement of 12 USC 1867(c)(2)—would cause little burden either for institutions or for the OCC. At least on a case-by-case basis, there are numerous ways the OCC might decide to use this collected information; but without collecting it the OCC certainly will be not be able to use it. (If the OCC decides not to change its existing approach, it will continue to learn about new provider relationships only on a delayed basis, at the time of an examination.)

2. <u>The TSP examination report for any regulated technology service provider should be made available to any financial institution that in good faith is considering hiring that service provider</u>.

The Federal banking regulators' current practice is to provide a copy of a service provider's TSP examination report *only to financial institutions that have already signed a contract* with the provider. This creates situations where an institution often *must sign a multi-year service contract* with a new provider (for legitimate reasons, from the provider's standpoint) without first knowing the contents of a TSP exam report that perhaps will provide a lot more insight, but only after the fact, into why the institution's already-binding decision is a good one or a bad one. By the time an institution is allowed to review a TSP exam report, that information gives no support to the institution's initial provider-selection process. The only provider-selection decision for which the report may then have any relevance is *a distant future decision whether to renew the newly-signed contract or not, when it expires.*

The last good chance for an institution to avoid being contractually bound to a less-than-satisfactory provider is actually before a contract is signed. Therefore, the most crucial point in time for an institution to learn what is disclosed in a TSP exam report is also *before the contract is signed.* As regulators have repeatedly emphasized, *an institution's management and its board of directors really need to make sure that adequate pre-contract due diligence has been performed on any proposed "critical activities" service provider; that risks have been appropriately considered; and that risks will be appropriately mitigated, before the institution selects that provider.* There is no good substitute for doing so.

Regulators are correct in expecting an institution's management and board to have sufficient information available and to evaluate it carefully before choosing "critical activities" vendors. But regulators also understand that community financial institutions in particular may have no choice but to outsource "critical activities." (An institution may lack the technical expertise or economies of scale to carry out these activities internally. At the same time, an institution's lack of internal technical expertise may limit its ability to analyze on its own the more technical details of any proposed service provider's operations and security controls.)

It would greatly assist community financial institutions if service providers would focus more attention on preparing and providing detailed "due diligence" information of the kind that these institutions need, especially relating to how the provider's services comply with bank regulatory requirements. But no amount of information provided by a vendor is ever sufficient in itself without some amount of further inquiry by the institution itself and, ideally, some source of *independent, objective technical analysis* confirming that the service provider's operations and security controls appear to be appropriate.

There are two potential sources of careful, independent, objective analysis of a service provider's operations that may be available to a community financial institution, without separate cost. These are in many respects the most important documents for a financial institution to obtain (if available). One of these unbiased sources of information is an SSAE 16 (SOC) audit report for the service provider (if one has been performed), prepared by an independent accounting firm. The other highly favored source of objective information is a TSP exam report prepared by the regulatory agencies. (Admittedly, what's contained in a TSP examination report is only part of what an institution should be reviewing before choosing a technology vendor—*but an institution is better off with it, than without it.*) If a SOC audit report and a TSP exam report could both be made available to an institution with respect to a proposed service provider, that institution would be less likely to make a poorly-considered vendor-selection decision, even if the institution has relatively little technical expertise internally.

Regulators can't make an institution's technology decisions—or even make strong recommendations. But that doesn't mean regulators have no stake in seeing these institutions reach good outcomes. TSP exams are already occurring, and it would be easy for the OCC to provide a TSP exam report to an institution before it makes a provider-selection decision. By doing so the OCC could significantly assist institutions in their process of making effective and informed provider-selection choices.

Regulated technology service providers should not be concerned about the fact that their TSP exam reports, including potentially confidential information about their operations, might be disclosed too freely to institutions that have not actually signed up with the provider. Regulators can alleviate any serious concerns by taking two simple preventive steps when providing a TSP exam report to an institution that is considering hiring a particular vendor: (1) Require the requesting institution to certify in good faith that it is requesting the exam report solely for the purpose of evaluating whether it should acquire that provider's services. (2) Warn the requesting institution strongly, similar to how institutions are warned concerning their own exam reports, that the information contained in the TSP exam report being provided by the regulators is confidential; that it cannot be used for any purpose other than for performing due diligence on the service provider; and that neither the report nor the information contained in it may be disclosed to any other person or entity.

3. The OCC should create a webpage (or distribute a periodic bulletin) listing the names of all regulated technology service providers.

Creating an informational webpage would assist any financial institution that is looking for a "critical activities" service provider, by allowing that institution to easily determine whether a specific service provider is receiving TSP exams. This proposed webpage need not include anything more than the names of technology service providers that currently are regulated and examined, and perhaps each provider's location. This amount of information, without more, is factual and should not be objectionable on any basis.

Whether or not the OCC decides to release a copy of a service provider's TSP exam report to a requesting financial institution before a contract is signed (as suggested above), it would still be helpful for institutions to have an easy reference like this suggested webpage, showing whether a TSP exam report will or will not be available for a particular provider if the institution signs a contract with that provider.

This suggested webpage should probably include some disclaimers or comments. Here is some possible language:

(1) The OCC neither recommends nor endorses any service provider. This list is provided only to disclose which technology service providers (TSPs) are currently receiving TSP examinations from the Federal banking regulatory agencies. Each of the TSPs on this list receives an examination rating, but the ratings are confidential and not disclosed publicly here. Any institution that signs a contract with a TSP listed here can contact the institution's primary Federal regulator to request a copy of that TSP's most recent TSP examination report.

As part of the TSP examination process, the regulatory agencies typically note any significant weaknesses in a regulated TSP's operations or security controls, and make recommendations for corrective action if the regulators deem that to be appropriate. (For any unregulated TSP, an institution may have a somewhat higher burden to carry out due diligence on its own, to learn more about whether that service provider's operations, security controls, and compliance with applicable regulatory guidelines are appropriate.)

(2) Financial institutions are reminded of the following language from OCC Bulletin 2013-29, *Risk Management Guidance*, dated October 39, 2013. The statements included below are applicable to circumstances including those where a financial institution may not have sufficient due diligence information in its files to allow examiners to form a reasonable conclusion as to a particular "critical activities" service provider's compliance with regulatory guidelines:

"When circumstances warrant, the OCC may use its authority to examine the functions or operations performed by a third party on the bank's behalf. Such examinations may evaluate safety and soundness risks, the financial and operational viability of the third party to fulfill its contractual obligations, compliance with applicable laws and regulations, including consumer protection, fair lending, BSA/AML and OFAC laws, and whether the third party engages in unfair or deceptive acts or practices in violation of federal or applicable state law. The OCC will pursue appropriate corrective measures, including enforcement actions, to address violations of law and regulations or unsafe or unsound banking practices by the bank or its third party. ***The OCC has the authority to assess a bank a special examination or investigation fee when the OCC examines or investigates the activities of a third party for the bank."***

BankOnIT believes the three suggestions outlined above would help to improve financial institutions' provider-selection process, as well as the OCC's ability to remain promptly aware of and to appropriately monitor these institutions' decisions regarding new "critical activities" and innovative services providers. We believe these suggestions are worthwhile for the OCC to review and implement. Thank you very much for your consideration.

Respectfully submitted,

\Charles Cheatham\

Charles Cheatham
SVP & General Counsel