MARKET INTEGRITY SOLUTIONS[LLC]

Washington, DC
October 18, 2021

Simultaneously submitted through the respective agency website portal to:

Office of the Comptroller of the Currency
Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation

Chief Counsel's Office
Attention: Comment Processing
Office of the Comptroller of the Currency
400 7th Street, SW
Suite 3E-218
Washington, DC 20219

Ann E. Misback
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

James P. Sheesley
Assistant Executive Secretary
Attention: Comments-RIN 3064-ZA26
Legal ESS
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429

Comment Letter to Proposed Interagency Guidance on

Third Party Relationships: Risk Management

OCC:	Docket ID OCC-2021-0011	
Federal Reserve System:	Docket No. OP-1752	
FDIC		RIN 3064-ZA26

Dear Sir or Madam:

We write in support of the purpose and the direction of, while also providing specific comments and further recommendations with respect to, the abovementioned Proposed Interagency Guidance as published in 86 Federal Register 38,183, dated July 19, 2021 (the "**Proposed Guidance**") by the Office of the Comptroller of the Currency ("OCC"), Board of Governors of the

Federal Reserve System ("Board"); and the Federal Deposit Insurance Corporation ("FDIC"), collectively referred herein as the "Federal Banking Agencies," for which the comment period was subsequently extended to October 18, 2021, as notified in 86 Federal Register 50,789, dated September 10, 2021.

Unless otherwise specifically indicated, the comments are directed equally to each of the OCC, Board, and FDIC. Furthermore, we believe it essential that such guidance not only be issued consistently across the Federal Banking Agencies, but specifically should also include the National Credit Union Administration. More broadly, the policy purpose behind the guidance would be better served by complementary efforts involving a broader group of Federal and State regulatory and supervisory authorities, and in coordination with foreign supervisory authorities who are currently increasing emphasis on the same subject matter areas.

II. Summary of Conclusion and General Comments

We write in support of the revisions in the Proposed Guidance.

Notwithstanding that the Proposed Guidance largely builds upon pre-existing principles, it is a positive step forward in a number of key respects, and could be made even more effective in reaching its goal of promoting sound banking practices by taking into consideration a few related concepts, as well as a few specific changes.

- The joint approach among the Federal Banking Agencies is welcome; there is no reason why they should have differing guidance on this subject.
- It is welcome that this guidance would replace pre-existing guidance; ongoing effort should be placed to revising regulatory pronouncements in this evolving area, withdrawing older materials, and noting relationships across related guidance and regulatory requirements.
- Specifically, this revision to the Proposed Guidance should take into consideration and be issued in connection with the Proposed Rulemaking on Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, published in 86 Federal Register 2299, dated January 12, 2021 (the "2021 Incident Notification NPRM").[1]
- The definition of "critical" should be more harmonized with other related regulatory pronouncements, and a specific suggestion is made below with respect to revision principles, including the incorporation of a risk materiality determination by individual banking organizations.
- The "Stages of the Risk Management Lifecycle" should more clearly add focus on the ties to operational resilience in the event of disruption by including common aspects of incident management such as proper communications.
- Subcontractor relationships and foreign based service parties are becoming more relevant and more challenging, with suggestions herein for more specific changes to the Proposed Guidance.
- Emphasis is appropriate on governance aspects, including the proper role of a board in overseeing risk management.

[1] OCC: Docket ID OCC-2020-0038, RIN 1557-AF02; Federal Reserve System: Docket No. R-1736, RIN 7100-AG06; FDIC: RIN 3064-AF59.

- The new additions to the Proposed Guidance in support of shared or collaborative approaches, or a utility, among financial institutions is appropriate and very welcome as these are shared challenges which will benefit in particular from allowing the sharing of commonly relied upon information and documentation, and reliance on collection by other parties.
- The Federal Banking Agencies are encouraged to consider the changes suggested in this common letter and from others contributing to the consultation, but should nonetheless move swiftly to finalize the guidance and ensure U.S. leadership towards harmonization of an area of focus by many regulators and supervisors globally.

III. About the Commenters

This comment is submitted by **Market Integrity Solutions, LLC**, a consulting firm providing executive advice on global financial regulation and innovative technology solutions. The primary author is Market Integrity Solution's founder, James H. Freis, Jr., a global expert in financial regulation, with a career dedicated to protecting the integrity of the financial markets. Mr. Freis was the longest-serving Director (CEO) of the United States Treasury Department's Financial Crimes Enforcement Network (FinCEN), the lead U.S. Government official for anti-money laundering and counter-terrorist financing requirements in close cooperation with the Federal Banking Agencies and other Federal, State and international financial sector supervisors. In addition to his experience working at the U.S. Department of the Treasury and the Federal Reserve Bank of New York, Mr. Freis served seven years at the Bank for International Settlements (BIS) in Basel, Switzerland, and six years with the Deutsche Börse Group based in Frankfurt am Main, Germany, with a leading global provider of systemically significant financial market infrastructures, where among other things he was a member of the executive leadership ensuring appropriate risk management over critical outsourcings in particular to technology service providers. He has most recently been associated with FinTech companies providing services including some of which would fall under the scope of the proposed notification requirements. Additionally, he has contributed to a separate comment letter being submitted on the Proposed Guidance by a company for which he is co-founder, CRINDATA LLC, which provides a SaaS platform with solutions for risk management of outsourcing to third party service providers.

IV. Responses to Request for Comment Questions

1. To what extent does the guidance provide sufficient utility, relevance, comprehensiveness, and clarity for banking organizations with different risk profiles and organizational structures? In what areas should the level of detail be increased or reduced? In particular, to what extent is the level of detail in the guidance's examples helpful for banking organizations as they design and evaluate their third-party risk-management practices?

The Proposed Guidance should more clearly relate to the operational resilience and business continuity aspects of risk management by introducing an additional phase in the Risk Management Life Cycle.

It is noted that the Figure 1: Stages of the Risk Management Life Cycle us unchanged from the 2013 OCC Guidance. That notwithstanding, as noted in the introduction to the Proposed Guidance, there is "increasing use of third parties" as a factual matter, and the proposed revisions provide more details as to risk management practices. In other words, volume and hence risk are up, and thus regulatory

expectations as to a bank's risk management response are also rising. Experience nonetheless suggests that many financial institutions are already lagging in their risk-based compliance with existing guidance for risk management of third party relationships. Thus, an expected reaction to the issuance of revised guidance, and the subsequent auditing and examination of compliance thereof, is processes that focus too much on checklists and administrative tasks and draw limited resources away from true risk minimization and recovery. Particularly as related to the factual observation of increased reliance on third party service providers overall, increased exposure equates to a higher probability of a disruption across the universe of service providers even if the risk is not necessarily higher in a specific bilateral relationship.

Effective risk management in support of safe and sound banking practices includes aspects of operational resilience and business continuity, areas of supervisory focus which have undergone significant evolution since the first issuance of guidance with respect to third party service provider oversight. In order for the Risk Management Life Cycle to be more comprehensive, it is proposed to expand the categories of the life cycle from five to six, by including a new operational resilience component after "ongoing monitoring" and before "termination."

Within this new "operational resilience" [alternative names could be considered] stage of the life cycles, the following aspects are suggested to be included:

- Cross-references to other operational resilience and business continuity guidance and supervisory policy and documentation
    - In this context it should be emphasized that the overall risk management approach with respect to third parties can raise awareness and minimize risks, but not eliminate them. As such, the full risk management life cycle must be integrated into such operational resilience and business continuity measures.
    - Note also that the European Banking Authority in its description of a risk management life cycle (albeit not presented in a graphical figure) includes business continuity planning.
- The aspect common to all operational incidents and to "oversight and accountability" of dealing with disruption is appropriate communication. This concept should be viewed in connection with the 2021 Incident Notification NPRM, and it is proposed that the revised guidance be implemented together with that rulemaking and appropriate cross-reference to the incident reporting be included within this new stage of the life cycle.
- The occurrence of an actual disruption incident is one of the most informative aspects of the entire risk management life cycle. It is suggested that this new stage of the life cycle include guidance that in the event of an incident involving a third party service provider, that a banking organization may wish to take this into consideration in revisiting or re-evaluating its risk assessment and risk tolerance with respect to the particular business activity and service provider, as well as further "lessons learned" to the extent applicable to its internal processes, or risk exposure to other service providers, including through subcontractors or in connection with concentration risk.

Adding the foregoing to the Proposed Guidance would be a very practical addition to true risk management, of a very practical rather than theoretical or more academic nature. Such an addition should also be connected with supervisory messaging that the changes to guidance remain an evolution

in thinking rather than a fundamentally different approach from the past, and should not lead to unintended consequences of disproportionate focus on administrative tasks that could detract from more productive risk management activities.

5. What changes or additional clarification, if any, would be helpful regarding the risks associated with engaging with foreign-based third parties?

The Proposed Guidance largely follows the 2013 OCC Guidance with respect to foreign-based third parties. As a practical matter, however, the factual exposure to foreign-based third parties has grown enormously, as visible in the following dimensions: the internationalization of financial markets; the growth of international activities and foreign presence of US financial groups; the corresponding growth of US activities of foreign financial groups; increased demand by customers for transactions and investors involving a foreign component; increased reliance on third parties to meet the foregoing demands; the growth and consolidation of service providers, particularly in the information technology sector; and the transformation of cloud-based solutions which are not necessarily limited to a particular jurisdiction. Financial institutions and groups are in many prudential areas required to apply a group or global rather than jurisdiction-based approach. Many service providers also seek to serve financial groups operating across multiple jurisdictions, or similarly to provider the same product or service offering to financial institutions individually based in different jurisdictions. Thus, the exposure to foreign service providers is up, while for many financial institutions they might have even less ability to influence the service offering or contractual terms of the service provider. As a result, guidance with respect to foreign-based third parties has taken on disproportionately larger relevance.

The 2013 OCC Guidance cautioned that contracts with foreign-based parties as compared to a fully US domestic context could be subject to different aspects of interpretation, adjudication and enforceability. The Proposed Guidance is slightly changed from recommending that a banking organization seek legal advice to "confirm", where in 2013 it was "to ensure", all aspects of a proposed contract with a foreign based third party. The Federal Banking Regulators are asked to clarify that this language is not meant to suggest that a formal written legal opinion is required in all cases and with respect to all aspects of a contract involving a foreign based third party, which could be expensive, time consuming, and difficult to obtain with a level of certainty as to "all aspects" on topics under an evolving regulatory environment. The guidance should clarify that a banking organizations should be able to take into consideration its level of familiarity and experience in dealing with a jurisdiction or service providers from a jurisdiction, for example if the financial institution have affiliates or a branch there.

The other change to the Proposed Guidance with respect to foreign-based third parties is that the legal advice should also be with respect to "other legal ramifications of each such business arrangement, including privacy laws and cross-border flow of information." This emphasis properly reflects significant change in the factual aspects of where data is held, including through a cloud provider; increased information collection, sharing, transparency or disclosure requirements on aspects such as tax status and beneficial ownership. It also reflects significant change in the legal requirements in this regard, be it through data protection and privacy regulations such as the EU General Data Protection Regulation; other prudential supervision requirements; or increased exercise of supervisory, judicial or police authority to access data held by a financial institution or third party service providers. The Federal Banking Agencies are encouraged to provide further guidance as to expectations for dealing with this

evolving area of risk. This should include incorporating and elaborating upon the bullet within he response to 2020 OCC FAQ number 11 ("Key areas of consideration for ongoing monitoring may include: … ◦ location of subcontractors and bank data.")

Finally, the Federal Banking Agencies are requested to include more detail to clarify expectations with respect to possible exposure to foreign-based third parties through the use of subcontractors. In particular, clarification is to be sought whether, and to what extent, due diligence, monitoring, or other measures across the risk management life cycle are to be applied to identify potential foreign exposure through third parties and their subcontractors. In this context, the bullet within the list of the "ongoing monitoring" obligations referring to location of subcontractors could be separated out to clarify expectations.[2] Not that exposure to foreign subcontractors could exist through domestic third party contractors that are not otherwise considered critical (under either the Proposed Guidance or the alternative suggested definition of "critical" as detailed below in response to question for comment number 8). Whereas identifying subcontractors and managing risks with respect to foreign-based third party service providers are each issues of challenge to banking organizations, the combination of subcontractors *and* foreign location is even more challenging. This issue would benefit from further guidance elaboration, and also is an area for which collaborative approaches and the use of utilities could be particularly beneficial.

6. How could the proposed guidance better help a banking organization appropriately scale its third-party risk management practices?

The OCC on August 27, 2021 published in OCC Bulletin 2021-40, "Third-Party Relationships: Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks" (the "2021 Community Bank Guide." The timing for this was somewhat surprising in light of the fact that the Proposed Guidance was recently out for consultation and that the 2021 Community Bank Guide noted its likely relevance to the broader outsourcing context.[3] "potential sources of information" and the "Illustrative Examples". It is thus proposed that it would be better to re-issue such a Guide as an annex of illustration in connection with the final version of the Proposed Guidance, to more closely align the heading with the Stages of the Risk Management Lifecycle, and to adopt additional illustrative examples for additional categories of third party service providers in addition to fintech companies. Said another way, a modular approach could be developed which would allow excerpting a summary of the full Guidance and supporting materials for a specific audience (e.g., community banks) and for a specific category of risk or service providers (e.g., fintechs or cloud-based solutions), but to nonetheless do so using the same structure as a more detailed guidance. Without such approach it can create more work

[2] See 86 Fed. Reg. at 38,195 ("A banking organization typically considers the following factors, among others, for ongoing monitoring of a third party: …

- Monitor the third party's reliance on, exposure to, performance of, and use of subcontractors, as stipulated in contractual requirements, the location of subcontractors, and the ongoing monitoring and control testing of subcontractors;") (emphasis added).

[3] See footnote 5 noting the consistency with the Proposed Guidance, and also introductory note for community banks: "Although the guide discusses community bank relationships with fintech companies, the content may be useful for banks of any size and for other types of third-party relationships."

and guessing for the banks to the extent each additional piece of guidance usually slightly different wording or an apparent need to compare against earlier pronouncements.

Additionally, we propose that revisions to the Proposed Guidance include materiality thresholds for critical activities which can be determined by the individual institution as set forth below in response to question for comment number 8.

8. In what ways could the proposed description of critical activities be clarified or improved?

The proposed description of "critical" activities could be clarified and improved by revising and applying more consistency across various related regulatory pronouncement a common definition of "critical." Secondly, the Federal Banking Regulators should promote prioritization of banking organization efforts towards risk management and mitigation by (i) defining specific activities which by default are critical, and (ii) service providers which even though critical do not require additional detailed application of the risk management guidance, such as due to lack of alternatives or existing supervisory oversight.

A. Definition of Critical – drawing from four supervisory sources

The Proposed Guidance expect more comprehensive and rigorous oversight and management of third-party relationships that support "critical activities." In turn, "critical activities" are defined as

> "significant bank functions" – whereby, "significant bank functions include any business line of a banking organization, including associated operations, services, functions, and support, that upon failure would result in a material loss of revenue, profit, or franchise value"
>
> or
>
> "other activities that:
>
> - could cause a banking organization to face significant risk if the third party fails to meet expectations;
> - could have significant customer impacts;
> - require significant investment in resources to implement the third-party relationship and manage the risk; or
> - could have a major impact on bank operations if the banking organization has to find an alternate third party or if the outsourced activity has to be brought in-house."[4]

In other contexts, the Federal Banking Agencies have used the word "critical" in a more limited context. For example, the October 2020 "Sound Practices to Strengthen Operational Resilience"[5] (the "2020 Operational Resilience Practices") albeit directed to the largest and most complex domestic banking organizations, contains constructive language, including in connection with its summary statements regarding managing risks with respect to third party service providers. Therein, "critical operations" are defined as "those operations of the firm, including associated services, functions and support, the failure or discontinuance of which would pose a threat to the financial stability of the United States." Hence,

[4] It is recognized that the latter portion of "other activities" component was in the OCC's 2013 guidance, with the proposal somewhat broadening the former component: "critical activities—significant bank functions (e.g., payments, clearing, settlements, custody) or significant shared services (e.g., information technology). . . "
[5] Available at https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-144a.pdf

this can be seen as a national systemic risk definition. The 2020 Operational Resilience Practices also defined as "core business lines" those "business lines of the firm, including associated operations, services, functions and support, that, in the view of the firm upon failure would result in a material loss of revenue, profit, or franchise value." Hence, there is risk of material loss. Instructively is the further definition of "tolerance for disruption": "Tolerance for disruption is determined by a firm's risk appetite for weathering disruption from operational risks considering its risk profile and the capabilities of its supporting operational environment. A firm's tolerance for disruption is informed by existing regulations and guidance and by the analysis of a range of severe but plausible scenarios that would affect its critical operations and core business lines." Tying this together, is the statement: "The firm identifies risks of third parties that provide it with public and critical infrastructure services, such as energy and telecommunications. The firm has processes to manage disruptions of these services and updates these processes as appropriate to stay within its tolerance for disruption."

As a third example, the 2021 Incident Reporting NPRM took a different approach. It noted that larger banking organizations subject to resolution planning requirements could use the classifications of critical operations already made in that context. The NPRM stated further, "However, the agencies do expect all banking organizations to have a sufficient understanding of their lines of business to be able to notify the appropriate agency of notification incidents that could result in a material loss of revenue, profit, or franchise value to the banking organization." In turn the NPRM suggested defining notification incident as an incident which:

> the banking organization believes in good faith could materially disrupt, degrade, or impair—
>
> (1) The ability of the banking organization to carry out banking operations, activities, or processes, or deliver banking products and services to a material portion of its customer base, in the ordinary course of business;
>
> (2) Any business line of a banking organization, including associated operations, services, functions and support, and would result in a material loss of revenue, profit, or franchise value; or
>
> (3) Those operations of a Banking organization, including associated services, functions and support, as applicable, the failure or discontinuance of which would pose a threat to the financial stability of the United States.

As a fourth and final example, the European Banking Authority's (EBA) 2019 Guidelines on Outsourcing Arrangements[6] define as "critical or important" a function "where a defect or failure in its performance would materially impair:"

i. the institution's continuing compliance with the conditions of their authorisation or its other obligations (including governance requirements with respect to which functions may be outsourced);
ii. their financial performance; or
iii. the soundness or continuity of their banking and payment services and activities.

[6] Available at: EBA BS 2019 xxx (EBA Draft Guidelines on outsourcing arrangements).docx (europa.eu)

Drawing from all of these sources, there are common factors as to what on a risk-basis can be considered "critical" activities:

- an **economic or financial** factor in terms of material loss to the banking organization
- a material disruption of **services to customers** (which might not necessarily lead to direct negative financial impact to the banking organization in the short-term)
- a failure to meet **specific regulatory requirements** (for example, disruption in a transaction monitoring function to identify possible financial crime risks)
- for a subset of larger institutions, activities deemed systemically significant in the context of existing resolution planning and related supervisory dialogue.

The first two of these factors could be addressed by determining materiality in connection with a banking organisation's own decisions as to its "tolerance for disruption" which could involve quantitative limits in percentage or absolute terms.

As compared to the OCC's 2013 Guidance and the Proposed Guidance, the following two components could be removed from the definition of "critical" and better integrated within the most pertinent Stages of the Risk Management Life Cycle. They are most relevant at the stages of planning and decisions to outsource or to maintain relationships:

- require significant investment in resources to implement the third-party relationship and manage the risk; or
- could have a major impact on bank operations if the banking organization has to find an alternate third party or if the outsourced activity has to be brought in-house.

It is thus suggested that these be removed from the definition of "critical activities" and integrated within those other life cycle components.

Hence, we propose that the Federal Banking Agencies address for revisions to this Proposed Guidance, and in connection with the 2021 Incident Reporting NPRM, and a more consistent approach to other related regulatory pronouncements going forward, these principles for activities, relationships and incidents deemed critical and therefore requiring an increased level of oversight and attention, in particular as related to the full like cycle of risk management with respect to third party service providers:

"Critical activities" are:

- a function or business line of a banking organization, including associated operations, services, functions, and support, the disruption of which would result in a material loss of revenue, profit, or franchise value;
- banking products and services, including associated operations, services, functions, and support, the disruption of which would negatively impact a material portion of its customer base, in the ordinary course of business

➢ for each of the foregoing two factors, materiality thresholds shall be determined by the management and subject to the risk management oversight by the board of directors;

- a material disruption to regulatory requirements with respect to safe and sound operations [this category would require additional supervisory clarification as to materiality]; and
- operations, including associated services, functions and support, the disruption of which would pose a threat to the financial stability of the United States, as identified in connection with resolution planning and supervisory guidance.

The foregoing would further risk-based, risk management practices.

B. Definition of Critical – drawing from four supervisory sources

Secondly, the Federal Banking Regulators should promote prioritization of banking organization efforts towards risk management and mitigation by (i) defining specific activities which by default are critical, and (ii) service providers which even though critical do not require additional detailed application of the risk management guidance, such as due to lack of alternatives or existing supervisory oversight.

Even with a more clear and consistent definition of "critical" being requested by multiple commentators, often with a materiality threshold, banking organizations will still require significant time and effort to characterize activities and third party service providers as critical. In certain cases, such effort could be better focused directly on risk management, oversight and mitigation rather than classification activities. The increasing detail in the Proposed Guidance, as well as the practical realities of audit and examination of thereof, does create obligations that could be the subject of relief. Practically, the Federal Banking Agencies could identify a range of activities or third party service providers which undoubtedly are critical such as the provider of a core banking system. Similarly, consistent with the third category in the above proposed definition could be identified by the Federal Banking Agencies such as transaction monitoring systems.

Furthermore, the Federal Banking Agencies are encouraged to provide guidance as to service providers that may be critical but for which the full application of the Proposed Guidance would not materially serve risk management purposes. For example, an exemption or exception could be applied with respect to financial market utilities subject to enhanced supervision. Similarly, consideration should be given to providing more guidance on what is expected of banking organizations with respect to oversight of other critical infrastructure providers such as telecommunications or electricity services. At the request of industry participants, the European Banking Authority clarified some of these type of exceptions from the application of its 2019 Outsourcing Guidelines.[7] With respect to financial market

[7] See paragraph 28 of the EBA Guidelines:

> As a general principle, institutions and payment institutions should not consider the following as outsourcing:
> a. a function that is legally required to be performed by a service provider, e.g. statutory audit;
> b. market information services (e.g. provision of data by Bloomberg, Moody's, Standard & Poor's, Fitch);
> c. global network infrastructures (e.g. Visa, MasterCard);
> d. clearing and settlement arrangements between clearing houses, central counterparties and settlement institutions and their members;
> e. global financial messaging infrastructures that are subject to oversight by relevant authorities;
> f. correspondent banking services; and
> g. the acquisition of services that would otherwise not be undertaken by the institution or payment institution (e.g. advice from an architect, providing legal opinion and representation in front of the court and administrative bodies, cleaning, gardening and maintenance of the institution's or payment institution's premises, medical services, servicing of company cars, catering, vending machine services,

utilities, such a step could elaborate further upon OCC FAQ 14 regarding reliance upon the disclosures from these utilities.

9. What additional information, if any, could the proposed guidance provide for banking organizations to consider when managing risks related to different types of business arrangements with third parties?

The Proposed Guidance should be revised to further clarify expectations for outsourcing business relationships within a banking or financial group, involving outsourcing to affiliates. We suggest that the guidance emphasize its overall applicability that a banking organization cannot outsource its responsibility for third party risk management. Nonetheless, a banking organization may be able to rely in particular on an affiliate or act together with others within a financial group on aspects such as planning, due diligence, monitoring and independent reviews. In turn, the guidance could emphasize that aspects of oversight and accountability or dealing with disruptions and notifications (see recommendations in response to question for comment number 1) remain with the banking organization and its management.

10. What revisions to the proposed guidance, if any, would better assist banking organizations in assessing third-party risk as technologies evolve?

As technologies evolve, so do the private sector as well as governmental authorities that the Federal Banking Agencies might view as credible authorities with respect to the risks and risk management in the use or exposure to such technologies, for example, NIST or FS-ISAC, or reporting formats, such as a SOC-1 or SOC-2 report. Without being prescriptive, it would be useful for the Federal Banking Agencies to draw industry attention to such credible authorities or recognized reporting formats. This could best be considered not just in general terms, but where applicable in "illustrative examples" or "potential sources of information" along the line of the OCC's August 2021 Community Bank Guide.

11. What additional information, if any, could the proposed guidance provide to banking organizations in managing the risk associated with third-party platforms that directly engage with end customers?

It would be useful to provide guidance as to expectations with respect to disclosure requirements (or if is clear there is not a disclosure requirement) to the end customers by either the banking organization or the third-party platform of the extent to which a banking organization's relationship is through a third-party platform directly engaging with the end customer.

12. What risk management practices do banking organizations find most effective in managing business arrangements in which a third party engages in activities for which there are regulatory

---

clerical services, travel services, post-room services, receptionists, secretaries and switchboard operators), goods (e.g. plastic cards, card readers, office supplies, personal computers, furniture) or utilities (e.g. electricity, gas, water, telephone line).

compliance requirements? How could the guidance further assist banking organizations in appropriately managing the compliance risks of these business arrangements?

See above response to question for comment number 8 suggesting that the Federal Banking Agencies provide guidance as to which regulatory compliance requirements should be considered "critical." As noted therein, other jurisdictions such as the European Union and its Member States have indicated certain regulatory compliance requirements that either cannot be outsourced to third party service providers, or which would require the enhanced oversight of critical relationships or activities.

13. In what ways, if any, could the discussion of shared due diligence in the proposed guidance provide better clarity to banking organizations regarding third-party due diligence activities?

Upon review of the Proposed Guidance as compared to the 2013 OCC Guidance, it is believed that the single aspect of the Proposed Guidance that is entirely new, albeit in part integrating other regulatory pronouncement including the 2020 OCC FAQs (including numbers 12 and 14), is the encouragement with respect to shared activities such as due diligence, and working with utilities, consortia, or standard-setting organizations. We encourage and applaud this, and recommend further elaboration and emphasis by the Federal Banking Agencies.

The most helpful aspect in which the guidance could provide better clarity and promote efficient and effective due diligence would be to specify expectations relating to the documentation and evidence requirements that would be subject to independent review, audit and examination of a banking organization's implementation of its risk management oversight activities. As a practical matter, banking organizations participating in shared due diligence activities should be able to rely on common evidence depositories to which they have access, rather than requiring them to download and separately file and maintain all aspects of documentation with respect to their due diligence. For example, some service providers directly, as well as utilities generally, make available to participating banking organizations standardized documentation that meets common needs of all participating banking organizations (e.g., annual reports and statements of financial condition, evidence of insurance, SOC-1 and SOC-2 reports, conclusions of audits, etc.). Such evidence might further involve documentation attesting to the absence of "negative news" whether the results of a monitoring check or audit or other third-party assessment. Part of an institution's participation in shared due diligence should include its ability to reasonably rely, consistent with its own risk tolerance, on monitoring or review by other parties that would only result in a type of alert or notification to the banking organization in the event of a material change. (In other words, there would be no need to "prove the negative" by documenting that a review or monitoring of the service provider did not indicate any change from the past or baseline review.)

14. In what ways, if any, could the proposed guidance further address due diligence options, including those that may be more cost effective? In what ways, if any, could the proposed guidance provide better clarity to banking organizations conducting due diligence, including working with utilities, consortiums, or standard-setting organizations?

We recommend that the emphasis on the opportunity for shared solutions, including working with utilities, consortia, or standard-setting organizations (regardless of the name or commercial arrangement so long as it is consistent with achieving this shared risk management goal), be emphasized

throughout the Risk Management Life Cycle, not merely in connection with the "due diligence and third-party selection" stage.

15. How could the proposed guidance be enhanced to provide more clarity on conducting due diligence for subcontractor relationships? To what extent would changing the terms used in explaining matters involving subcontractors (for example, fourth parties) enhance the understandability and effectiveness of this proposed guidance? What other practices or principles regarding subcontractors should be addressed in the proposed guidance?

Here are three suggestions for enhancements with respect to subcontractor relationships.

First, the most important practices and principles to address with respect to subcontractors would be providing guidance on levels of materiality or criticality that require attention from banking organizations. It is not sufficient guidance to say that matters involving further subcontractors should be risk-based, especially to the extent that (i) there is already a challenge for banking organizations to gather relevant insights with respect to subcontractors with whom they have no direct relationship; (ii) third party service providers are not necessarily applying the same level of consideration as banking organizations to the nature of their relationships with subcontractor third party service providers; and (iii) as noted throughout this guidance but in particular in response to question 8, the Federal Banking Agencies employ different definitions of "critical" in different pronouncements. Further guidance as to which subcontractor relationships deserve a type of enhanced due diligence as well as which could involve none, minimal or simplified due diligence could help banking organizations better prioritize their efforts and thus be more effective in their risk management.

Second, the exercise of the Federal Banking Agencies of their existing authority over third party service providers, in particular under the Bank Service Company Act, would also help banking organizations by making the service providers more understanding of, and receptive to, risk management efforts consistent with this Proposed Guidance. A good example of this is to issue together with revisions to this Proposed Guidance regulations in furtherance of the requirements on service providers under the 2021 Incident Notification NPRM.

Third, the Proposed Guidance should more clearly on a stand-along basis articulate the notion of "concentration risk" in connection with or *caused by* subcontractors. To illustrate the point, a banking organization might have a primary service provider as well as a backup service provider for a particular service. If each of those two service providers rely directly or indirectly on the same critical subcontractor, then there is a potential single point of failure for the service notwithstanding otherwise good faith attempts towards business continuity and operational resilience of having a primary and backup provider. The notion of "concentration risk" is understood in theory and a matter of concern globally among banking supervisors, but a challenge in practice, as recently confirmed through a public consultation by the Financial Stability Board.[8] Furthermore, there is a lack of timely and granular data

[8] See Financial Stability Board, "Regulatory and Supervisory Issues relating to Outsourcing and Third-Party Relationships: Overview of Responses to the Public Consultation" (June 14, 2021), at 3, available at: https://www.fsb.org/wp-content/uploads/P140621.pdf .

available to supervisors with respect to concentration risk. In the Proposed Guidance, there is a clear statement to take into consideration concentration risk with respect to direct relationships with third party service providers: "Additionally, a banking organization may be exposed to concentration risk if it is overly reliant on a particular third-party service provider." In contrast, with respect to *indirect* subcontractors, this point is somewhat lost in the following broader sentence: "Evaluate whether additional risks may arise from the third party's reliance on subcontractors and, as appropriate, conduct similar due diligence on the third party's critical subcontractors, such as when additional risk may arise due to concentration-related risk, when the third party outsources significant activities, or when subcontracting poses other material risks."[9]

We thus propose that the portion of the guidance with respect to subcontractors include a distinct sentence or point to raise awareness that concentration risk may arise not only through directly reliance on a particular third-party service provider, but also indirectly or cumulatively due to the subcontracting chain. Ideally, this would be understood in the context of the first recommended practice and principle as to materiality of the subcontracting relationship (meaning that if the contribution to the service provided is immaterial from a risk perspective, then it would also not contribute cumulatively to concentration risk). It is further noted that identifying such concentration risks would be substantially aided by banking organizations relying on an industry collaborative institution or utility, which could also help regulators and supervisors identify concentration risks not only for individual regulated entities but which also could pose systemic financial stability concerns due to the potential impact of a disruption simultaneously affecting multiple banking organizations.[10]

The preambulatory section "F. Subcontractors" immediately proceeding question for comment number 15 uses the term "chain" of subcontractors three times. That notwithstanding, the word "chain" does not appear anywhere in the Proposed Guidance. We recommend that it should, because it is a visually descriptive term, and would help emphasize that there could be more than one subcontractor in any

---

> **Concentration risk.** Many respondents mentioned that concentration of critical services in the same third-party service provider by financial institutions may create risks to the financial system. These risks become greater if the service or product provided by the relevant third party is difficult to substitute (see also "substitutability" below). In addition, a number of respondents highlighted the inability of financial institutions to monitor systemic concentrations in the provision of third-party services as they do not have access to data on other financial institutions' dependencies on specific third-party service providers. Moreover, some services, including certain "niche" services, are provided by a very small number of third-party service providers, and are therefore by their nature concentrated. According to many of these respondents, identifying, monitoring and managing systemic concentration risk in the provision of third-party services and other interdependencies is beyond the responsibility of individual financial institutions. A number of respondents also cautioned against unduly complex or prescriptive requirements to address concentration risk (e.g. a requirement on financial institutions to use multiple vendors) as they could place a disproportionate burden on institutions' operational capacity.

[9] See Proposed Guidance section 2.A.n "Reliance on Subcontractors".

[10] See also excerpt from Financial Stability Board

given third party relationship. There can even be "chains of chains," and risks are not limited to the concentration risk aspect noted in the immediately preceding paragraph.

Regarding terms involving subcontractors, we recommend *against* the use of the term "fourth parties". This neither provides clarity (it is an ambiguous term), nor can it be understood from other contexts outside of this Proposed Guidance. On the latter point, note that there is already an inconsistency in the longstanding use of the term "third party", which as a legal matter is understood to a non-party to a contract who nonetheless may be affected by a contractual relationship. Thus from a legal perspective a customer would be a third party affected by a contractual outsourcing relationship by the customer's bank to a service provider implementing services for the customer. It is already inconsistent from a formal legal perspective to have a very significant portion of the existing outsourcing guidance and in the middle stage of the Risk Management Lifecycle to focus on "contract negotiation" between a banking organization and a "third party". Thus, please do not refer to fourth parties, which furthermore can involve a chain of subcontractors (fifth or sixth parties?).

The term subcontractor, or in the European Union, also "sub-outsourcer" is clearer and more commonly understood, including that there could be multiple layers of further subcontractors or sub-outsourcers down the chain of service providers. Even in the general public there is an understanding of a common example of a house renovation overseen by a "general contractor" who in turn will bring in specialist subcontractors such as an electrician, plumber, and other service providers.

Please also note the comments in response to question 5 with respect to foreign third parties, in particular the last paragraph with respect to exposure to foreign subcontractors.

16. What factors should a banking organization consider in determining the types of subcontracting it is comfortable accepting in a third-party relationship? What additional factors are relevant when the relationship involves a critical activity?

Please see response to question 15.

18. To what extent should the concepts discussed in the OCC's 2020 FAQs be incorporated into the guidance? What would be the best way to incorporate the concepts?

All of the concepts discussed in the OCC's 2020 FAQs should be incorporated into the Proposed Guidance, and those FAQs should subsequently be withdrawn. Specific comments as to how to incorporate some of the individual FAQs may be found above in response to questions for comment numbers 5, 8, 13, and 14.

V. Incorporation by Reference of Other Comments

We hereby incorporate by reference the attachment hereto, which is a comment letter dated April 12, 2021 on the Proposed Rulemaking on Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, published in 86 Federal Register 2299, dated January 12,

2021 (the "2021 Incident Notification NPRM").[11] As stated herein, we believe that the Proposed Guidance should be revised and issued in conjunction with a final rule, revised consistent with comments to that NPRM. Moreover, that earlier comment letter contains additional material, including about policy considerations and international developments, relevant to the Proposed Guidance.

Secondly, a distinct comment letter on the Proposed Guidance is being filed on behalf of CRINDATA LLC. The authors of this comment letter agree with and support the issues raised in the CRINDATA submission.

VI. Closing

Thank you for the opportunity to comment on the Proposed Guidance, and related important policy objectives.

Sincerely,

Market Integrity Solutions, LLC

By: *James H. Freis, Jr.*
James H. Freis, Jr.
Founder

[11] The full references to that NPRM are found above at footnote 1. The prior public comment letter was submitted to each of the Federal Banking Agencies, and may be found at, for example through the comments to the OCC, at https://www.regulations.gov/comment/OCC-2020-0038-0017.

Washington, DC
April 12, 2021

Simultaneously submitted through the respective agency website portal to:

Office of the Comptroller of the Currency
Board of Governors of the Federal Reserve System
Federal Deposit Insurance Corporation

Comment Letter to Notice of Proposed Rulemaking

Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers

OCC:	Docket ID OCC-2020-0038	RIN 1557-AF02
Federal Reserve System:	Docket No. R-1736	RIN 7100-AG06
FDIC		RIN 3064-AF59

Dear Sir or Madam:

We write in support of the purpose and the direction of, while also providing specific comments and further recommendations with respect to, the abovementioned Notice of Proposed Rulemaking as published in 86 Federal Register 2299, dated January 12, 2021 (the "NPRM") by the Office of the Comptroller of the Currency ("OCC"), Board of Governors of the Federal Reserve System ("Board"); and the Federal Deposit Insurance Corporation ("FDIC"), collectively referred herein as the "Federal Banking Agencies." Unless otherwise specifically indicated, the comments are directed equally to each of the OCC, Board, and FDIC; moreover, we believe it essential that such a regulatory proposal not only be implemented consistently across the Federal Banking Agencies, but also that the policy purpose would be better served by complementary efforts involving a broader group of Federal and State regulatory and supervisory authorities.

I. Executive Summary of Conclusion

The first notification requirement by a banking organization to its primary Federal regulator as an "early alert" is reasonable and appropriate, and will further the missions of the Federal Banking Agencies as well as serve with minimal costs incrementally to help protect individual banking organizations and potentially against broader financial stability risks. The second notification requirement for bank service providers is also reasonable, and in fact is a necessary prerequisite for the banking organizations relying on such services to carry out effective risk management as well as more effectively fulfilling the banking organizations' own notification requirement. It is also reasonable to have these two distinct notification requirements, because it is correct that bank service providers generally are not in a position to evaluate the potential impact for their banking organization customers. For example, the same service

offering could be critical to one banking organization in terms of profits and customer utilization, but entirely marginal to the business of another banking organization. (A subset of service providers such as for a core banking system might more easily assume that an incident would be material to its customers.) It is also reasonable for the Federal Banking Agencies to expect initial notifications to be provided within a relatively short period of time. One of the major change in connection with technological innovation is to provide financial services with faster services (e.g., real-time payments); thus an incident can immediately have an impact, and supervisors rightfully would wish for an initial early alert, long before they might be able to expect a more detailed impact analysis which will be specific to the incident.

While it is understandable that the Federal Banking Agencies frame these proposed notification requirements in significant part under the authority of the Bank Service Company Act – in particular related to notification of service relationships and examination authority for contract providers – such framework is not consistent with the way either banking organizations or their service providers manage potential risks with respect to their relationship. As a result, the second notification requirement as proposed is not well defined in its scope, and could be made more effective through further clarification in relation to complementary outsourcing risk management requirements, for which there is additional precedent, and ongoing initiatives, including current international efforts that should be instructive.

II. About the Commenters

This comment is submitted by **Market Integrity Solutions, LLC**, a consulting firm providing executive advice on global financial regulation and innovative technology solutions, and by **RS Technologies, LLC**, a FinTech company (Mark Stetler, CEO) providing anti-money laundering solutions to the banking industry. The primary author is Market Integrity Solution's founder, James H. Freis, Jr., a global expert in financial regulation, with a career dedicated to protecting the integrity of the financial markets. Mr. Freis was the longest-serving Director (CEO) of the United States Treasury Department's Financial Crimes Enforcement Network (FinCEN), the lead U.S. Government official for anti-money laundering and counter-terrorist financing requirements in close cooperation with the Federal Banking Agencies and other Federal, State and international financial sector supervisors. FinCEN is also the agency responsible for collecting, analyzing, and disseminating Suspicious Activity Reports (SARs) from banking organizations, and Mr. Freis agrees with and confirms the discussion in the NPRM that such SAR reporting does not fulfill the purpose sought under the NPRM.[1] In addition to his experience working at the U.S. Department of the Treasury and the Federal Reserve Bank of New York, Mr. Freis served seven years at the Bank for International Settlements (BIS) in Basel, Switzerland, and six years with the Deutsche Börse Group based in Frankfurt am Main, Germany, with a leading global provider of systemically significant financial market infrastructures, where among other things he was a member of the executive leadership ensuring appropriate risk management over critical outsourcings in particular to technology service providers. He has most recently been associated with FinTech companies providing services including some of which would fall under the scope of the proposed notification requirements.

Mr. Stetler is co-founder and CEO of RS Technologies, LLC and RegSmart, a FinTech Company founded in 2016 providing automated anti-money laundering risk management solutions to the community bank

[1] FinCEN's guidance regarding SARs in connection with cybersecurity incidents is also inapposite. See FinCEN Advisory - FIN-2016-A005 | FinCEN.gov

market. He was previously senior partner in NIA Consutling, which was among the largest financial forensic audit audit firms that served the mortgage origination and mortgage servicing markets founded in 1985.

Messrs. Freis and Stetler have evaluated options for technology solutions which could fulfill the proposed notification requirements of the NPRM in an efficient and cost-effective way, while also fulfilling broader policy interests and considerations as discussed in this comment letter. On the basis of our relevant experience and that specific analysis, we conclude that the overall benefits of the proposed notification requirements would exceed the overall costs.

III. Summary Views on Policy Objectives and Other Relevant Initiatives

We strongly support the policy direction of this NPRM, which should result in:

- Increased focus *by banking organizations* on the evolving risks of their reliance on bank service providers and outsourcing more generally, which increasingly involves technology service providers;
- Greater awareness and responsiveness *among the class of bank service providers* in working with banking organization in terms of preparatory planning for possible service outages, as well as in response to incidents; and
- Greater insight *of financial supervisors* over risks to individual institutions, as well as more broadly across regulated banking organizations and their service providers, in particular through risks of concentration on certain providers or sub-contractors.

In order **to make this regulatory framework more effective**, the Federal Banking Agencies should:

- Align the NPRM and guidance thereunder not merely with the relatively obscure provisions of the Bank Service Company Act, but rather more closely with the body of complementary regulatory expectations relating to **outsourcing, in particular with respect to technology service providers**;
  - This can be achieved in a practical way through more detailed focus on the proposed new definition of bank service provider, which as currently drafted does not provide sufficient notice to, or clarity about, the entities subject to the new obligations;
- Emphasize that while this initiative largely reflects risks related to technology developments, that banking organizations should not misinterpret these obligations narrowly in terms of cybersecurity, but rather more importantly from the perspective of the **impacts upon their business** (again, reminiscent of outsourcing more broadly);
- Develop these specific regulations in the context of overdue modernization of the outsourcing guidance and related regulatory expectations, for which **insights can be drawn from evolving international norms**;
- While respectful of the limitations of the authority of the Federal Banking Agencies and not wishing to delay their initiative in this regard, **coordinate with other Federal and State financial supervisors**, particularly due to the fact that a significant number of underlying bank service providers are likely to also contract with financial services providers not

licensed by the Federal Banking Agencies, which in turn would complement the policy purpose and benefits sought by the Federal Banking Agencies.

Regarding the **specific reporting obligations proposed** in the NPRM, we believe:

- ✓ The proposed notification requirements are **not sufficiently covered by existing regulatory obligations** (in particular those with respect to outsourcing which are not sufficiently fulfilled in light of the evolving risk);
- ✓ **Focus should be on areas of higher risk**, not all service provider relationships, which again parallels the risk-based focus of outsourcing management; and
- ✓ The implementation of a structure for the notification requirements, both on behalf of banking organizations and bank service providers, lend themselves to a type of **industry initiative or shared approach**, rather than ad hoc measures by each entity, which approach would not only be **more efficient and effective** but would also better facilitate the Federal Banking Agencies' objective of gaining insights into broader financial stability risks.

IV. Proposed Notification Requirements Can Be Most Efficient and Effective in Complement to Other Policy Initiatives

A. Impact upon Business Operations

We recommend that the Federal Banking Agencies more clearly emphasize that while this initiative largely reflects risks related to technology developments, nonetheless, banking organizations should not misinterpret these obligations narrowly in terms of cybersecurity, but rather more importantly from the perspective of the **impacts upon their business**. The definition of "notification incident" makes clear that the focus involves impact on business operations, yet the NPRM preamble introduction begins with a discussion of the more narrow issue of cyberattacks. Care should be taken with the rollout of any final regulation that responsibility for these issues should best be in connection with management and board responsibility for business critical outsourcings, as described further below.

B. Relevance to FinTech Oversight and White-labelled Services

More generally, one of the more pressing regulatory challenges spurred by technological innovation are initiatives of companies which may be categorized broadly as "FinTechs." Some FinTech companies may seek to employ technology to provide one or more aspects of financial services in a more efficient and cost-effective way by employing modern technology to thereby compete with or to "disrupt" traditional financial services providers and/or aspects of their business models. Such companies might fall under regulatory and licensing requirements on a functional basis, particularly as they expand the range of products or services offered, in some cases eventually seeking a banking license.

Increasingly, however, many FinTechs are partnering with (or even being acquired by) traditional banking organizations or other licensed financial services providers. Certain FinTechs are likely falling within the scope of the Bank Service Company Act and its examination authority, as well as the NPRM's proposed notification requirements for bank service providers. Moreover, many banking organizations are increasingly relying on specialized external parties offering components of banking as well as permissible non-banking services which, as discussed below in the comment with respect to NPRM item 10 definition of bank service companies, also fall within the scope of the Bank Service Company Act. The

Federal Banking Agencies are urged to consider the foregoing as part of their overall approach and available "toolbox" to risk mitigation related to emerging technology innovations by banking organizations, their service partners, and new types of competitors.

C. Coordination with Other Interested Supervisory Authorities

The policy interests underlying the NPRM are not unique to the Federal Banking Agencies nor the banking organizations supervised by them. Rather, multiple other Federal and State financial supervisors have shown similar interest, and it would further the financial stability interests of the Federal Banking Agencies if complementary initiatives were advanced. Moreover, a significant number of underlying bank service providers are likely also to contract with financial services providers not licensed by the Federal Banking Agencies, meaning that the greatest systemic risks could better be addressed by a coordinated approach, in particular involving the confidential exchange of information among regulators with respect to risks and incidents.

A bill before the current U.S. Congress, the Bank Service Company Examination Coordination Act, H.R. 2270 (introduced March 26, 2021), following upon similar proposals introduced in previous Congresses, would expand coordination and information with State banking supervisors. The passing of this legislation and its ensuing implementation would further the purpose of the NPRM. Such coordination is particularly appropriate in light of the fact that the majority of States already have examination authority similar to that of the Federal Banking Agencies.[2] State regulators also serve as primary licensing authorities for a range of financial services providers, including insurance companies and money transmitters, which may serve as critical service providers to entities licensed by the Federal Banking Agencies.

The Federal Banking Agencies already coordinate interagency programs to supervise third-party servicers through the Federal Financial Institutions Examination Council (FFIEC).[3] The National Credit Union Administration (NCUA) does not have independent regulatory authority over technology service providers.[4] Consideration could also be given to formalizing such authority for the NCUA, as there is no reason why its supervisory interests should diverge from those of the Federal Banking Agencies; if anything, credit unions are at least if not more reliant on external service providers than many banks.

Reference is also made to the notification requirements under the Securities and Exchange Commission's (SEC) Regulation Systems Compliance and Integrity (Regulation SCI) which was developed, *inter alia*, in light of the dependency of the securities markets on evolving technology and vulnerabilities to outages including in connection with cyberattacks.[5] Notably, a covered entity is required both to

---

[2] See Press Release dated March 26, 2021 of Congressman Roger Williams of Texas announcing the reintroduction of the Bank Service Company Examination Coordination Act (BSCECA) of 2021 (attributing to Texas Department of Banking Commissioner Charles Cooper that thirty-eight States have the authority to examine banks' third-party service providers), available at Rep. Williams Increases Coordination Between State and Federal Banking Regulators | Congressman Roger Williams (house.gov).

[3] See FFIEC IT Examination Handbook, Supervision of Technology Service Providers (TSP) Booklet (October 2012) at endnote 1, available at FFIEC IT Examination Handbook InfoBase - Supervision of Technology Service Providers.

[4] See *id.*

[5] See SEC Final Rule, Systems Compliance and Integrity, 79 Fed. Reg. 72,252 (December 5, 2014), as implemented in particular in 17 CFR § 242.1002--.1007, available at 2014-27767.pdf (govinfo.gov). The primary author of this

make an "immediate" notification to its Federal regulator of an incident; followed within 24 hours on a "good faith, best efforts basis" by a notification of event and assessment to the extent available at that time; and at later times more detailed impact assessments.[6] This approach is generally consistent with the "early alert" approach in the NPRM of the immediate notification by a bank service provider, and subsequent notification by a banking organization after it believes in good faith that a reportable incident has occurred. While as compared to the NPRM of the Federal Banking Agencies, the SEC Regulation SCI is much broader in content while more limited in application to certain of its regulated entities,[7] the more detailed framework of Regulation SCI is more appropriate for Financial Market Utilities (FMUs) – this responds to the NPRM request for comment item 6 about unique factors in how best to apply notification requirements to FMUs.

The primary author of this comment letter, in his role as former FinCEN Director, can personally attest to his direct, successful experience in coordination, as well as delegating regulatory examination experience to State authorities, in addition to the Federal Banking Agencies and other Federal financial services regulators. We believe that while the Federal Banking Agencies should proceed with this proposal, they should seek continually to expand coordination and appropriate information sharing relevant to risks with a broad range of other Federal and State regulators. Such complementary efforts would better promote the purpose of the NPRM, and also close potential gaps in understanding possible risks to financial stability as well as opportunities for regulatory arbitrage. While it is believed that the multiple licensing and chartering opportunities in the U.S. financial system can promote competition and in turn innovation, the ability to manage critical dependencies and deal with incidents is an area for regulatory cooperation, not for regulatory competition (such as a race to the bottom). Cooperation would serve to level the playing field for relevant risks, and promote financial stability oversight through a more comprehensive view of risks, especially in light of underlying technology providers servicing multiple classes of licensed entities.

D. Draw Upon Complementary Outsourcing Risk Management Framework

The NPRM's content is very closely related to the regulatory expectations of the Federal Banking Agencies with respect to outsourcing risk management, yet there is no material reference thereto in the NPRM.[8] "Outsourcing" is defined in the FFIEC IT Examination Handbook as: "The practice of contracting through a formal agreement with a third-party(ies) to perform services, functions, or support that might otherwise be conducted in-house."[9] The first paragraph of the introduction to the FFIEC IT Booklet entitled "Outsourcing Technology Services" is very similar to the policy interests expressed in the NPRM:

> The financial services industry has changed rapidly and dramatically. Advances in technology enable institutions to provide customers with an array of products, services, and delivery channels. One result of these changes is that financial institutions increasingly rely on external

---

comment letter previously had oversight responsibility for the implementation of Regulation SCI by SEC regulated exchanges.

[6] See 17 CFR § 242.1002(b).

[7] See 79 Fed. Reg. at 72,256 (noting SEC estimate of 44 entities being subject to the SCI proposal).

[8] The term "outsourcing" only appears once in the NPRM. See 86 Fed. Reg. at 2308 ("The Board is unable to estimate the number of bank service providers that are small due to the varying types of banking organizations that may enter into outsourcing arrangements with bank service providers.").

[9] See Glossary definition of "Outsourcing", available at FFIEC IT Examination Handbook InfoBase - Glossary

> service providers for a variety of technology-related services. Generally, the term "outsourcing" is used to describe these types of arrangements.[10]

The Federal Banking Agencies also do not in the NPRM make reference to their guidance (notably more narrow than the scope of the BSCA) specific to technology aspects of bank service providers: the 2012 FFIEC IT Examination Handbook on "Supervision of Technology Service Providers"[11] (the "TSP Booklet").

Albeit somewhat dated, the Outsourcing Technology Services Handbook contains critically important principles in light of the NPRM's focus on the business relevance of proposed "notification incidents." The first section of that Handbook following the introduction states:

> The responsibility for properly overseeing outsourced relationships lies with the institution's board of directors and senior management. Although the technology needed to support business objectives is often a critical factor in deciding to outsource, managing such relationships is more than just a technology issue; it is an enterprise-wide corporate management issue. An effective outsourcing oversight program should provide the framework for management to identify, measure, monitor, and control the risks associated with outsourcing. The board and senior management should develop and implement enterprise-wide policies to govern the outsourcing process consistently. These policies should address outsourced relationships from an end-to-end perspective, including establishing servicing requirements and strategies; selecting a provider; negotiating the contract; and monitoring, changing, and discontinuing the outsourced relationship.

The NPRM's proposed notification requirement would appear to be a minor additional step upon a banking organization's robustly implemented outsourcing framework.

There is, however, ample reason to doubt that banking organizations having consistently implemented the existing outsourcing requirements, certainly at the level of the above-quoted management and board attention, and in light of the evolving reliance on technology and breadth of contracted services. Note, for example, the evaluation results of the FDIC Office of Inspector General:

> *We did not see evidence, in the form of risk assessments or contract due diligence, that most of the FDIC-supervised [financial institutions (FIs)] we reviewed fully considered and assessed the potential impact and risk that [technology service providers (TSPs)] may have on the FI's ability to manage its own business continuity planning and incident response and reporting operations.* Typically, FI contracts with TSPs did not clearly address TSP responsibilities and lacked specific contract provisions to protect FI interests or preserve FI rights. Contracts also did not sufficiently define key terminology related to business continuity and incident response. As a result, FI contracts with TSPs we reviewed provided FIs with limited information and assurance that TSPs (1) could recover and resume critical systems, services, and operations timely and effectively if

[10] Available at: FFIEC IT Examination Handbook InfoBase - Introduction. Compare NPRM, 86 Fed. Reg. at 2302 ("As technological developments have increased in pace, banks have become increasingly reliant on bank service providers to provide essential technology-related products and services.")

[11] Available at: FFIEC IT Examination Handbook InfoBase - Supervision of Technology Service Providers; references herein to the TSP Booklet are to the .pdf version available at ffiec_itbooklet_supervisionoftechnologyserviceproviders.pdf.

> disrupted; and (2) would take appropriate steps to contain and control incidents and report them timely to appropriate parties.[12]

The FDIC subsequently advised regulated institutions of ongoing observations of deficiencies in this regard.[13]

V. International Financial Regulatory Focus on Outsourcing and Technology Risks

While the Federal Banking Agencies were early adopters and proponents of requirements that banking institutions manage risks related to outsourcing and, in particular, technology services providers, the U.S. guidance could be updated in light of the emerging supervisory norms, including as relevant to the notification requirements in the NPRM. More recent outsourcing guidance has generally been narrower, such as related to cybersecurity and cloud services, but the NPRM seeks to focus on broader risks.

The FFIEC issued its Technology Examination Handbook (IT Handbook) "Outsourcing Technology Services Booklet" (booklet) in June 2004.[14] This significantly influenced the first global effort among financial supervisors in guidance issued by the Joint Forum in 2005.[15] On November 9, 2020, the Financial Stability Board (FSB) issued for public consultation a discussion paper on the topic of "Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships," largely building upon the framework established in the 2005 Joint Forum guidelines.[16] The context of the FSB consultation was the financial industry's increasing reliance on third parties, particularly in the area of technology, with challenges further accelerated through the COVID-19 experience. Common themes raised by multiple comments in response to the consultation include:

- advocating the need for a coordinated supervisory approach, including more consistent definitions of key terms, particularly on a cross-border basis;

---

[12] See FDIC Office of Inspector General, Report No. EVAL-17-004, "Technology Service Provider Contracts with FDIC-Supervised Institutions" (February 2017) (emphasis added), available at: Technology Service Provider Contracts with FDIC-Supervised Institutions | Federal Deposit Insurance Corporation Office of Inspector General (fdicoig.gov)

[13] See FDIC, Financial Institution Letter FIL-19-2019 (April 2, 2019) entitled "Technology Service Provider Contracts":

> Examiners have noted in recent FDIC reports of examination that some financial institution contracts with technology service providers may not adequately define rights and responsibilities regarding business continuity and incident response, or provide sufficient detail to allow financial institutions to manage those processes and risks.

[14] Available at ffiec_itbooklet_outsourcingtechnologyservices.pdf. Note also the introductory paragraph as consistent with the risks indicated over sixteen years later in this NPRM:

> The financial services industry has changed rapidly and dramatically. Advances in technology enable institutions to provide customers with an array of products, services, and delivery channels. One result of these changes is that financial institutions increasingly rely on external service providers for a variety of technology-related services. Generally, the term "outsourcing" is used to describe these types of arrangements.

[15] The report is available at Outsourcing in Financial Services (bis.org). Note that the primary author of this comment letter was working at the Bank for International Settlements during the development of this report.

[16] https://www.fsb.org/2020/11/regulatory-and-supervisory-issues-relating-to-outsourcing-and-third-party-relationships-discussion-paper/

- practical difficulties (or the potential for unrealistic expectations) related to sub-outsourcings (sometimes referred to a "fourth-party" issues), particularly in a service provided in a common way to multiple customers; and
- potential conflicts with data localization initiatives or efforts to limit cross-border transfers of data.

Regarding the challenges for financial institutions overseeing their risks with third-party providers, banking associations advocated possible mitigants through: joint industry audits, direct supervisor oversight of third party service providers, or development of certification schemes. While going beyond the scope of the NPRM, **the policy objectives of this consultation and the comments in response are consistent with those being pursued by the Federal Banking Agencies. The consultation and comments also lend support to the main themes of this comment letter** that the specific NPRM proposal must be considered in the context of other domestic and global complementary initiatives; and, that the second notification requirement with respect to bank service providers needs to better articulate the affected entities in order to improve its effectiveness.

The most important specific new regulatory requirements in another jurisdiction related to outsourcing are the European Banking Authority's (EBA) 2019 publication of the "EBA Guidelines on Outsourcing Arrangements."[17] While not specifying notification requirements akin to the NPRM (which would be within the purview of regional and national supervisors), in addition to the general outsourcing context, we wish to draw attention to the definitions of critical outsourcing and to the focus on sub-outsourcing.

In the NPRM, the Federal Banking Agencies suggest the ability of certain banking organizations to rely upon their resolution planning for identifying core business lines and critical operations; in contrast, banking institutions not subject to the Resolution Planning Rule are not required to identify these solely for the purpose of the proposed notification requirements. "However, the agencies do expect all banking organizations to have a sufficient understanding of their lines of business to be able to notify the appropriate agency of notification incidents that could result in a material loss of revenue, profit, or franchise value to the banking organization."[18] The EBA Guidelines have requirements with respect to the identification and risk management of outsourcing of "critical or important functions" which include meeting licensing obligations; affecting a bank's financial performance; or the soundness or continuity of their banking and payment services.[19] The second and third points in the EBA Guidelines are consistent with the first two prongs of the notification incident definition. To the extent the Federal Banking Agencies choose to focus the notification requirements to areas of greater risk or a materiality standard, it would be useful to consider the evolving understanding of critical outsourcings, such as consistent with the EBA Guidelines.

Sub-outsourcing, as noted in each of the FSB consultation and the EBA Guidelines, is an evolving area of concern and also challenge for all parties concerned: supervisors, banking organizations, and bank service providers. This issue goes beyond the scope of the notification proposals in the NPRM, but it is

[17] https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf?retry=1
[18] See 86 Fed. Reg. at 2303.
[19] See EBA Guidelines, paragraph 29.

mentioned in that the Federal Banking Agencies, as part of a more holistic approach to understanding and addressing outsourcing risks, should give future attention to this topic.

The international examples should not merely be considered as an examples, but rather are directly relevant to various aspects of an effective approach by the Federal Banking Agencies, including because:

- many banking organizations that would be subject to the proposed rules are also subject to these foreign regulations; and particularly with respect to critical outsourcing may fall under groupwide risk management approaches; and
- many of the bank service providers, including global leading technology service providers, also service non-U.S. institutions.

VI. Responses to Specific "Request for Comment" Items

In addition, to the foregoing comments on various aspects of the proposal, we wish to provide detailed comments with regard to items 5 and 10, and targeted comments on items 11 and 13, as well as the Paperwork Reduction Act provisions.

Cross-reference

Please refer to the above discussion of SEC Regulation SCI in the subsection entitled "3. Coordination with Other Interested Supervisory Authorities" as relevant to **comment item 3** (SEC requires 24 hours for regulated entities; as the Federal Banking Agencies oversee a larger number of smaller entities it appears reasonable to extend this time period to 36 hours); comment item **4** (noting that the SEC already uses a "good faith" standard, hence supporting its reasonableness in this NPRM); comment item **6** (relevance for FMUs); and comment item **12** (immediate notification of initial issue is consistent with the SEC framework).

Comment Item 5. Notification to the Federal Banking Agencies

The Federal Banking Agencies should support the development of, and reliance by banking organizations and by bank services providers, on collaborative solutions to meet their notification obligations, including standardized reporting formats. In the event of a computer-security incident giving rise to time-critical notification, based on the short timelines, there is no ability to then consider what if any reporting notifications might arise. Each reporting entity should be able to evidence on an ongoing basis that it has structured processes and procedures; responsible and accountable personnel; and reliable communications channels in place to the meet the notification requirements, review of which should be included as appropriate in supervisory examinations.

Regarding how to provide notifications, and to whom at the Federal Banking Agencies, it is recommended that notification be made electronically, in writing and subject to recordkeeping and audit trail. Such communication should be made to one central point of contact, ideally using a shared service such as under the auspices of the FFIEC, but at a minimum to one central notification node within each Federal Banking Agency. Such central point of contact should in turn be responsible for disseminating to responsible persons within the agency or among cooperating supervisory authorities. (The foregoing would not preclude, for example, a banking organization from promptly informing its primary contact(s) in its specific supervisory team(s), but it is recommended that the regulatory requirement for notification be met through notifying a central agency point of contact.)

We also recommend with respect to the communications channels for delivering notifications:

- for all parties involved – be it a bank service company (or its sub-contractor), a banking organization, or a regulator; the notification obligation should be as automated as possible and not interrupt in particular the subject matter expert individuals or managers who should be focusing their attention on remediation or mitigating the risks of the computer-security incident, which by definition raises potentially material risks for the banking organization; and
- because bank service providers generally are expected to provide services for multiple banking organizations, it must be assumed that a computer-security incident could impact multiple banking organizations, thus requiring multiple notifications; as a matter of efficiency, a collaborative notification system would be more efficient than bilateral communications.

Consideration should also be given to the fact that in the event of a computer-security incident impacting a bank service provider, the normal communication channels of such bank service provider to its customer banking organization might also be interrupted. For example, if the bank service provider provides externally hosted software services, the banking organization might in the normal course receive ongoing reporting about the functioning of that service. In the event of a computer-security incident that might generically be referred to as an outage – equivalent to a total software outage or interruption of connectivity lines or power outage – this could also effectively take offline the normal communication channel from the bank service provide to the banking organization. As another example, if the computer-security incident involved an interruption by the bank's internet service provider, the bank might not be able to use its normal electronic communications channels with its regulators. Hence, in all cases, consideration should be given to a type of business continuity measure, or alternate reporting channel, for each of bank service providers and banking organizations to make their notification requirements under the proposed rules.

The Federal Banking Agencies need not be prescriptive with respect to the content or means of the notification (separate from providing a central point of contact). Rather, this is a good opportunity for industry to come up with efficient solutions and improve them over time.

Comment Item 10. Proposed definition of "bank service provider"

The definition of "bank service provider" in the proposed rule is not sufficiently clear. An ambiguous definition risks, first, that the "other persons" providing services under contract to a banking organizations do not have sufficient notice that the Federal Banking Agencies are applying by regulation the NPRM's notification obligations upon them, thus raising questions of due process and fairness, while also potentially undermining the purpose of those obligations. Secondly, banking organizations face ambiguity with respect to which of their contractual service providers are intended to fall within the obligations under the rule, again risking undermining the policy purpose.

The term "bank service provider" has not previously been defined in the Code of Federal Regulations, nor is it a specifically defined term such as in relevant FFIEC examination handbooks. The proposed definition is:

> *Bank service provider* means a bank service company or other person providing services to a banking organization that is subject to the Bank Services Company Act (12 U.S.C. 1861-1867).[20]

The subset of "bank service company" is a reasonably defined class in light of the BSCA definition based on ownership by a banking organization and the supervisory oversight and approval in connection with such ownership.[21] The ambiguous part of the proposed definition is "other person providing services to a banking organization that is subject to the Bank Services Company Act." The term "banking organization" is defined in the proposed rule immediately proceeding and the scope of this definition is separately the subject of requests for comments numbers 6, 7, and 8 of the proposed rule. Thus, the ambiguous phrase can be further reduced to clarify the presumed meaning of the determiner "*that*": "other person providing services … subject to the Bank Services Company Act."

From the year 1962 when the Bank Service Company Act ("BSCA") was adopted with its references to "bank services," there has been significant expansion in the allowable business of banking. This has occurred through distinct legislative amendments as well as regulatory interpretations; and, furthermore, the application of these authorities to evolving technology supporting financial services. In short, the BSCA itself contains language from a legacy era (e.g., with respect to checks and their physical mailing) predating modern financial services; and is focused primarily on the more limited allowable services for companies owned by regulated banking organizations.[22] The more relevant issues for the purpose of the NPRM are how the Federal Banking Agencies from a modern technology perspective interpret the 12 U.S.C. § 1863 language of "any other clerical, bookkeeping, accounting, statistical, or similar functions performed for a depository institution" being permissible for a bank service company *or performed under contract*, in each case subject to examination under 12 U.S.C. § 1867.[23] One of the more recent (2019) interpretations of the FDIC, notes that services "similar" to those enumerated in the BSCA provision (otherwise unchanged since its adoption in 1962) include "Internet banking, or mobile banking services."[24]

---

[20] The proposed definition language is identical in each of proposed OCC § 53.2(b)(2); Board § 225.301(a) [note this is not numbered as subsection (a)(2) as internally cross-referenced in proposed § 222.300(c)]; and FDIC § 304.22(b)(2).

[21] See, e.g., 12 CFR § 5.35 (describing the procedures and requirements regarding OCC review and approval of a notice by a national bank or Federal savings association to invest in the equity of a bank service company).

[22] See 12 U.S.C. § 1861(b) (defining "bank service company").

[23] Note that the opinions expressed herein are meant to apply also with respect to services performed by savings association service companies, subsidiaries or by contract, subject to similar oversight as under the BSCA, in accordance with 12 U.S.C. § 1464(d)(7).

[24] See FDIC, Financial Institution Letter FIL-19-2019 (April 2, 2019) entitled "Technology Service Provider Contracts", referring to the BSCA notification requirements, available at fil19019.pdf (fdic.gov):

> Section 7 of the Bank Service Company Act (Act) (12 U.S.C. 1867) requires depository institutions to notify, in writing, their respective federal banking agency of contracts or relationships with technology service providers that provide certain services. Services covered by Section 3 of the Act include check and deposit sorting and posting, computation and posting of interest, preparation and mailing of checks or statements, and other clerical, bookkeeping, accounting, statistical, *or similar functions such as data processing, Internet banking, or mobile banking services*.

(emphasis added).

Cf. the original language of the BSCA, Pub. L. 87-856:

> (b) The term "bank services" means services such as check and deposit sorting and posting, computation and posting of interest and other credits and charges, preparation and mailing of checks, statements,

The preamble to the NPRM suggests that the Federal Banking Agencies intend the definition "bank service provider" to be applied broadly to a range of modern contractual services providers.[25] The NPRM text accompanying footnote 14 quotes the antiquated language of the BSCA, and notes that the bank services subject to the BSCA also include "components that underlie these activities."[26] The NPRM continues: "Other services that are subject to the BSCA include data processing, back office services, and activities related to credit extensions, as well as components that underlie these activities."[27] Footnote 15 further details that such services must be permissible for bank holding companies under the Bank Holding Company Act and implementing under 12 CFR § 225.28, listing the fourteen categories of nonbanking activities which have been defined and refined over decades as "so closely related to banking or managing or controlling banks as to be a proper incident thereto," and therefore permissible to be engaged in by a bank holding company or its subsidiary.[28] The last such subcategory of permissible nonbanking activities is "data processing," described in that regulation as:

> (i) Providing data processing, data storage and data transmission services, facilities (including data processing, data storage and data transmission hardware, software, documentation, or operating personnel), databases, advice, and access to such services, facilities, or data-bases by any technological means, if:
>
> > (A) The data to be processed, stored or furnished are financial, banking or economic; and
> >
> > (B) The hardware provided in connection therewith is offered only in conjunction with software designed and marketed for the processing, storage and transmission of financial, banking, or economic data, and where the general purpose hardware does not constitute more than 30 percent of the cost of any packaged offering.[29]

The point of the foregoing is to illustrate that **the simple proposed definition in the NPRM of "bank service provider" has insufficient clarity as to the intended scope of the regulation**, without reference first to contractual service providers subject to examination under the BSCA, and second to permissible nonbanking activities under the Bank Holding Company Act – areas of detail known only to regulatory specialists.

The policy direction underlying the NPRM suggests that the regulators should wish to more clearly provide notice of the application to technology service providers (TSPs) to banks. The NPRM preamble description of the second aspect of the proposal requiring a bank service provider to notify banking organizations of a computer security incident states: "As technological developments have increased in pace, banks have become increasingly reliant on bank service providers to provide essential technology-related products and services."[30] In the NPRM Impact Analysis, the Federal Banking Agencies note that

---

notices, and similar items, or any other clerical, bookkeeping, accounting, statistical, or similar functions performed for a bank.

[25] See 86 Fed. Reg. 2301, note 6 ("Bank service providers would include both bank service companies and third-party providers under the BSCA.").

[26] 86 Fed. Reg. 2302, note 14.

[27] 86 Fed. Reg. 2302.

[28] 86 Fed. Reg. 2302, note 15; see also 12 CFR § 225.28.

[29] 12 CFR § 225.28(b)(14)(i).

[30] 86 Fed. Reg. 2302.

they "do not have data on the number of bank service providers that would be affected by this requirement."[31] They provide an estimate through reference to the North American Industry Classification System (NAICS) industry code 5415, "Computer System Design and Related Services." Separate from the number of affected parties, this reference provides further indication of a relevant target group for the regulation, as distinct from the myriad other services which fall under the cascade of the BSCA reference.

The FFIEC TSP Booklet includes the identification and selection of TSPs warranting interagency supervision and the development of a risk-based supervisory strategy for each of these entities. That approach provides for examination coverage of selected TSPs, including the non-exclusive list of core application processors, electronic funds transfer switches, Internet banking providers, item processors, managed security servicers, and data storage servicers.[32]

NPRM request for comment item 10 regarding the definition of "bank service provider" also requests comment on which bank service providers, or which services should be subject to the notification requirements. We suggest that as an administrative matter the regulation text for the notification requirement on bank service provider should be drafted broadly, but the Federal Banking Agencies **should provide guidance** (which can be amended or updated from time to time) with a non-exclusive list of **categories of bank service provider subject to the regulation**. This should include in one place each of the classes of service providers mentioned in the foregoing sources referenced in this comment letter which reflect past regulatory determinations of the Federal Banking Agencies of relevance to the purposes of the proposed rule. Without such transparency, however, it would not be rational to expect that such bank service providers had received effective notice of the intended application of the new proposed rule, which would undermine its policy effectiveness.

Comment Item 11. Notification of all, or only affected, banking organizations

We believe that bank service providers should err on the side of cautious in notifying any banking organizations that *might* be affected by an incident. In this context, it must be understood, that the bank service provider would not necessarily be expected "immediately" to have a full understanding of the impact of the incident. That being said, the notification requirement in the NPRM should not require the bank service provider to notify entities of incidents which the bank service provider reasonably believes are limited to unrelated entities, such as a data access or corruption issue limited to the data of one banking organization. The exclusion of such limited incidents from the notification requirement under the NPRM should not be viewed as preventing a banking organization customer from learning generically about the statistical reliability of a particular service provided to the banking sector.

Comment Item 13. How best to notify at least two individuals at banking organizations

We do not believe that all bank service organizations currently have sufficient processes to carry out the proposed regulatory requirement for timely notification to their banking organization customers of an incident. In particular, as described above, an outage impacting the service could also impact the bank

[31] 86 Fed. Reg. 2304.

[32] See TSP Booklet at 6, and note 12, available at: FFIEC IT Examination Handbook InfoBase - Supervision of Technology Service Providers; page citation is to the .pdf version available at ffiec_itbooklet_supervisionoftechnologyserviceproviders.pdf.

service provider's normal means of communication with the banking organization customer. Therefore, the communications channel planned for meeting such notification requirement should also contemplate appropriate business continuity measures or alternative channels. Regarding the proposal to notify at least two individuals at affected banking organizations, we propose that the most efficient and best option on the side of each of the bank service provider and the banking organization is to agree a central point of contact at the banking organization which would be accessible by more than one person to ensure that notifications to the banking organization are timely received and acted upon. This could best be accomplished by a structured process involving written communications (likely a standardized incident message), rather than naming two individuals or involving telephone communication.

Also, the proposed notification requirement for bank service providers would apply for an incident "for four or more hours." This time element, however, appears superfluous, as the notification applies to a "computer-security incident" which is proposed to be defined as an occurrence that results in actual or potential harm or constitutes a violation or imminent threat of violation of security policies. We suggest that, if the Federal Banking Agencies consider alternative definitions of incident, the time element could be one factor that alone would require notification to a banking organization if the service were unavailable more than four hours. Other material risks, such as potential data loss or compromise, should be subject to notification requirements regardless of the time element. The NIST framework provides other guidance to establishing materiality thresholds for notification.

Comments with respect to the Paperwork Reduction Act elements

We believe and posit:

(a) for the reasons stated above, the collections of information are necessary for the proper performance of the agencies' functions, and, yes, the information has practical utility to the Federal Banking Agencies;

(c) + (d) regarding ways to enhance the quality, utility, and clarity of the information to be collected; and ways to minimize the burden of the information collections on respondents, including through the use of automated collection techniques or other forms of information technology; please see the response to comment item 5 above regarding notification to the Federal Banking Agencies.

VII. Closing

Thank you for the opportunity to comment on this proposed rulemaking, and related important policy objectives.

Sincerely,

Market Integrity Solutions, LLC

By: *James H. Freis, Jr.*
James H. Freis, Jr.
Founder