www.CRINDATA.com

October 18, 2021

Chief Counsel's Office
Attention: Comment Processing
Office of the Comptroller of the Currency
400 7th Street, SW
Suite 3E-218
Washington, DC 20219
RE: OCC Docket ID OCC-2021-0011

Ann E. Misback
Secretary
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551
RE: Federal Reserve System Docket No. OP-1752

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

*Simultaneously submitted through the respective agency's website portal*

Comment Letter to Proposed Interagency Guidance on
**Third Party Relationships: Risk Management**

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. This comment letter will provide more detailed comments on the following aspects.

1. The importance of an aligned and consistent message among the Federal Banking Agencies, ideally to be further supported by other supervisors.
2. In January 2021, the Federal Banking Agencies published for public comment a Proposed Rulemaking on Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers (the "**2021 Incident Notification NPRM**").[1] We believe that that the finalization of that rulemaking would significantly advance the policy objectives also behind the Proposed Guidance, and believe that each of the proposed rulemaking and this Proposed Guidance should be revised consistent with comments and then issued concurrently in final form.
3. Incident notification and related communications are among the aspects of business continuity management and operational resilience activities which should be included in an additional component to the "Stages of the Risk Management Lifecycle" as described in the Proposed Guidance and Figure 1.
4. The definition of "critical" should more closely follow the related definitions within the 2021 Incident Notification NPRM.
5. Revisions to the Proposed Guidance should place further emphasis upon the risk of subcontractor chains (or subcontractors' sub-subcontractors).
6. Shared solutions are appropriate and can be viable, effective, and efficient not only at the level of due diligence, but throughout the risk management life cycle. The Proposed Guidance should be revised to provide more clarity in this regard and give greater comfort to banking organizations to adopt a variety of shared solution approaches to facilitate third party service provider risk management.

[1] See 86 Federal Register 2299 (January 12, 2021), OCC: Docket ID OCC-2020-0038, RIN 1557-AF02; Federal Reserve System: Docket No. R-1736, RIN 7100-AG06; FDIC: RIN 3064-AF59.

## III. About the Commenters

This comment is submitted by **CRINDATA**, LLC, (www.CRINDATA.com) which offers solutions to financial institutions for managing operational risk in their reliance on third party service providers. CRINDATA offers unique cloud-based solutions to financial institutions who must pro-actively manage their critical third-party relationships (including their indirect relationships with subcontractors) and must prepare for and mitigate business disruptions management and cybersecurity events originating anywhere in the chain of service providers and subcontractors. Concurrently, CRINDATA helps third party service providers like core systems, payments providers, transaction motoring solutions, banker's banks, and corporate credit unions, by substantially simplifying the due diligence interactions with financial service companies and by providing a compliant, common platform and communications to manage business disruptions and cybersecurity events when they occur. The platform serves needs across multiple jurisdictions applying similar, evolving risk management principles.

The primary authors of this comment letter are CRINDATA's co-founders, CEO Mark Stetler and Chairman James H. Freis, Jr. Mr. Stetler, is also 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 market. He was previously senior partner in NIA Consulting, which was among the largest financial forensic audit audit firms that served the mortgage origination and mortgage servicing markets founded in 1985. Mr. Freis, also founder of the consulting firm Market Integrity Solutions, LLC, was formerly Director (CEO) of the United States Treasury Department's Financial Crimes Enforcement Network (FinCEN), and previously served at the Federal Reserve Bank of New York, the Bank for International Settlements, and the Deutsche Börse Group's financial market infrastructures.

## IV. General Comments – Promote Further Harmonization

We believe it a very important step for the Federal Banking Agencies to adopt on a harmonized basis the Proposed Guidance. This should include the integration of the 2020 OCC FAQs. Furthermore, this trend should continue with respect to related aspects of operational risk management. In turn, older guidance should be withdrawn or rescinded. There is no reason to differentiate on the basis of banking organization charter (and hence supervisor) among risk management principles applicable to third party service providers. This statement is consistent with requiring individual banking organizations to make risk-based determinations with respect to their specific facts and circumstances.

Moreover, the Proposed Guidance should be joined by the National Credit Union Administration (NCUA). We understand that the in the context of the 2021 Incident Notification NPRM that the NCUA may not have the same or analogous authority to impose regulatory obligations upon, or to examine, third party service providers within the scope of the Bank Service Company Act or analogous authority applicable to savings associations. That nonetheless should not limit the

NCUA from agreeing to apply the principles in the proposed guidance to credit unions. Moreover, State banking supervisors could also join the Proposed Guidance in include its principles in their respective oversight of State-licensed institutions, consistently with the FDIC and Federal Reserve System.

More consistent application is not only merited because the categories of risks together with prudent risk management considerations apply universally across all charter types. Moreover, many third party service providers (including general IT service providers and fintechs) increasingly seek to provide products, services and solutions with respect to financial institutions of multiple charter types. These service providers should not be subject to differing regulatory expectations either directly or as applied but their financial institution customers.

Harmonized regulatory expectations will also promote critical mass for the development of shared solutions, consortia, and utilities as encouraged in the Proposed Guidance. A larger market of potential financial institution and third party service providers seeking risk management solutions will also promote more innovation by solution developers and providers, and common costs can be broadly shared, thus lowering the costs for compliance and effective risk management for all participants.

As a secondary step, greater benefits in cost-efficient and effective risk management could be achieved by encouraging shared approaches on a cross-border basis. For instance, this could be promoted by encouraging broader adoption of the principles in the Proposed Guidance by the Financial Stability Board in furtherance of its November 2020 consultation on outsourcing risk management. Effectively, this could be seen as a modernization of the work of the Federal Banking Agencies almost two decades ago in promoting third party risk management by banking supervisors globally. Other foreign supervisors have recently been very active in this area of third party service provider risk management, in particularly within the EU, where the European Banking Authority's 2019 Outsourcing Guidelines, implemented in turn by EU Member State regulations, are meant to go into full effect by the end of 2021, and the European Securities and Markets Authority (ESMA) has more recently issued a series of related guidance. We have not observed significant differences in underlying principles that would prevent greater harmonization among global regulators.

## V. 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 be strengthened by including more context and cross-references to related guidance regarding responsibilities in the event that a risk materializes, such as a disruption to a service provided by a third party. How a banking organization responds to such a risk incident, in particular a critical one, is an essential part of a Risk Management Life Cycle.

As such, the existing Stages of the Risk Management Life Cycle in Figure taken from the 2013 OCC Guidance is materially incomplete. Currently, the life cycle and its description represents appropriate risk management preparation, but includes few aspects of prudent practices when a risk actually materializes.

The 2021 Incident Notification NPRM would fill part of that gap if issued on a harmonized basis in connection with the revised guidance. It is recommended not to issue the revised guidance without also finalizing the incident notification rulemaking.

Once the incident notification regulation is issued, this could be incorporated as part of a new, additional stage of the Risk Management Life Cycle which would directly refer to the importance of timely incident notification, and could more generally reference broader guidance on aspects of business continuity management and operational resilience. In areas of operational risk other than with respect to relationships with third party service providers, aspects of resiliency have been supervisory priorities in recent years. So too should they be with respect to risks of increasing reliance on third party service providers, at a minimum with respect to critical activities and services.

Moreover, increased focus on incident notification and communication in particular, would strengthen other aspects of the Risk Management Life Cycle, and more specifically the sides of the triangle in Figure 1. They are a component of the "Documentation and reporting" axis; and are essential to the exercise of "Oversight and accountability" among corporate governance bodies. Moreover, arguably the best indication through "Independent reviews" as to whether policies and procedures to meet regulatory requirements and promote safety and soundness are reasonably designed and implemented is to observe their application with respect to true incidents. "Lessons learned" from actual incidents (or experience with incidents shared among banking organizations participating in a shared solution) should inform possible revisions to overall risk management policies and procedures, and also lead to the re-assessment of the risk of relying on a particular third party service provider (i.e., triggering an ad hoc review). Please integrate these observations into revisions of the guidance in the Risk Management Life Cycle.

We also note in favor of pursuing the 2021 Incident Notification NPRM, the increasing focus among financial institutions, customers, and supervisory authorities of "timeliness." This reflects the factual evolution of the financial industry as it evolves from paper-based instruments and physical interaction at bricks-and-mortar banks, to electronic interaction, and increasing services towards real-time payments and instant or near-instant execution. Thus, a category of outage or business disruption for a specific length of time (e.g., a number of hours), could have a much greater negative impact than a similar disruption a matter of years ago when fewer financial transactions were highly time sensitive. One of the small changes in the Proposed Guidance from the 2013 OCC Guidance is the introduction of the word "timeliness" within the due diligence factors for third party service provider selection, with respect to k. "Incident

Reporting and Management Programs."[2] Finalizing that proposed rulemaking to require timely notifications by each of the service provider to the financial organization and the financial organization to its supervisor would further this policy emphasis in the Proposed Guidance.

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

In an increasingly globalized world, there is more cross-border activity than ever before. While financial institutions generally are subject to jurisdiction-based licensing and oversight in order to deliver financial services in particular to individual consumers, this is much less the case for many third party service providers. That being said, third party service providers to regulated financial institutions are increasingly subject to oversight by banking supervisors at least as related to delivery of services to banks under their oversight (equivalent to the Bank Service Company Act). The Federal Banking Agencies should consider developing guidance as to foreign jurisdictions in which third party service providers are subject to analogous oversight. This could take the form of a type of "equivalence" determination. Alternatively, in jurisdictions from which there is no analogous oversight, a banking organization generally would be expected to apply a higher level of scrutiny and due diligence before making a decision to outsource to such service provider.

Second, it should be recognized when a banking organization relies on either its own direct experience (e.g., in its cross-border operations or among affiliates within a group), or that of a consortium of respected banking organization counterparts in considering the reliability of a foreign-based third party service provider. All the benefits of shared solutions – including due diligence, contracting, ongoing monitoring, audits, etc. – could be even more valuable and efficient for a banking organization to manage risks with respect to foreign based service providers. We recommend that the Proposed Guidance include a specific statement to this effect.

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

The Federal Banking Agencies should adopt a harmonized and more consistent definition of "critical" not only in the Proposed Guidance but also in related regulatory documentation. Moreover, they should start by providing lists of those activities and relationships for which there is a presumption of being critical (a core system) or not critical (an ancillary product offering). This presumption nonetheless can be rebuttable or subject to challenge to take into consideration all relevant facts and circumstance so as to remain risk-based. After the application of this rebuttable presumptive list, banking organizations would be required to apply

[2] See 86 FR at 38,190: "Review and consider the third party's incident reporting and management programs to ensure there are clearly documented processes, **timelines,** and accountability for identifying, reporting, investigating, and escalating incidents." (emphasis added).

a risk-based approach taking into consideration multiple factors, in particular negative effects upon its customers and the potential for economic loss to the banking organization.

In this regard, the 2021 Incident Reporting NPRM is instructive in determining which types of incident would require notification. That definition focused on the potential for: (1) material disruption to a products and services to a material portion of its customer base; and (2) a material loss of revenue, profit, or franchise value; with a final factor of the more extreme risk of a threat to national financial stability. Many commenters to the NPRM suggested that the Federal Banking Agencies clarify a materiality threshold to the first two aspects; in so doing, this would provide practical guidance to banking organizations as to the focus on risk management with respect to the impact of third party service providers.

*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 it 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.

*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?*

The concept of shared due diligence—and sharing of aspects of the broader risk management life cycle notwithstanding individual risk determinations—is very important and a welcome addition to the Proposed Guidance as compared to the 2013 OCC Guidance. It is logical that parallel approaches to obtain and analyze background documentation as well as ongoing monitoring of risk indications with respect to the same service offering to multiple banks could lend itself to shared solutions. Such share solutions would lessen duplication of effort, reduce costs, and allow better deployment of resources with respect to other aspects of risk management. Moreover, we have evaluated and developed options for technology solutions which could facilitate the due diligence requirements of the Proposed Guidance in an efficient and cost-effective way. Notwithstanding the logical appeal, however, banking organizations still have quite limited experience in operationalizing shared solutions, so more detailed guidance would speed adoption and, thus, the policy goals of risk management.

We recommend that answers to the following practical questions, and other suggestions, be included in a new section of the guidance with respect to shared solutions:

- In the bilateral exercise of due diligence, a banking organization generally would obtain responses to due diligence inquiries (e.g., documentation or representations) directly from a third party service provider. What are the expectations or requirements for a banking organization to rely on information or documentation obtained through a shared solution?

(For example, what level of verification or "audit trail" is necessary from the shared solution provider?)

- Shared solutions might not have the same documentation (including comprehensive responses to an institution's own due diligence questionnaire). It is suggested that the guidance adopt a principle that in participating in shared solutions, banking organizations may make a risk-based determination that the information obtained through the shared solution is reasonably sufficient to make a decision, even if not complete or identical with the information which would have been sought under the banking organization's own bilateral practices and procedures.
- If shared solutions provide a banking organization with ongoing access to documentation or information, may a banking organization refrain from downloading and maintaining all available documentation in duplicate files? May the shared solution thus also serve to meet recordkeeping that evidences aspects of due diligence activities?
- Please include a statement that shared solutions with respect to due diligence may also be applied with respect to ongoing monitoring obligations, specifically monitoring to identify material changes to the facts identified through the due diligence, such as negative news indications.

*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?*

As stated in the explanatory paragraph preceding questions for comment numbers 13 and 14, we agree that the benefits of working with shared solutions apply beyond due diligence: "banking organizations may be able to collaborate when performing due diligence, negotiating contracts, and performing ongoing monitoring." We recommend that the Proposed Guidance specifically include this broader application of shared solutions.

As to the nature of the shared solutions, we agree that this might include various types such as utilities, consortiums, or standard-setting institutions. It should be understood that the shared solutions might also take the form of a commercial provider that leverages a risk management solution by licensing or selling the service to multiple banking organizations which would benefit from receiving the service at a lower cost than if the banking organization were to conduct the activity itself. To best express this, the Federal Banking Agencies should make clear that a banking organisation's decision to rely on a shared third party risk management solution could be justified by similar cost-benefit calculations as to any other third party service provider, and also would be subject to the application of this guidance in managing the risks of that outsourcing. By raising the notion of a "consortium" or "utility", the Federal Banking Agencies should not limit a shared solution to any particular corporate form nor require any specific type of banking organization contribution in order to benefit from the solution. Furthermore, reliance on specialized third party service provider of this type of risk management solutions would be

consistent with the provision in the Proposed Guidance under "Independent reviews" for "Confirming that conflicts of interest or appearances of conflicts of interest do not exist when selecting or overseeing third parties."

While we recommend generally that the 2020 OCC FAQs be integrated fully into the Proposed Guidance (and the FAQs then be withdrawn to avoid confusion), some of the FAQs are particularly instructive with respect to banking organizations pursuing shared solutions. FAQ 12 notes, "If they are using the same service providers to secure or obtain like products or services, banks may collaborate to meet certain expectations, such as performing the due diligence, contract negotiation, and ongoing monitoring responsibilities described in OCC Bulletin 2013–29." The foregoing sentence corresponds to the second, third and fourth stages of the Risk Management Life Cycle. FAQ 14 notes, "Banks can also rely on pooled audit reports, which are audits paid for by a group of banks that use the same company for similar products or services." This corresponds to the "independent reviews" on the left side of the triangle in the figure depicting the Stages of the Risk Management Life Cycle.

We also support the addition to the Proposed Guidance with respect to the right side of the triangle in the figure depicting the Stages of the Risk Management Life Cycle. An addition beyond the OCC's 2013 Guidance within section 4. Guidance and Accountability, states that proper "d. Documentation and Reporting" may include, according to the new, last bullet: "Reports from third parties of service disruptions, security breaches, or other events that pose a significant risk to the banking organization." Anecdotally, there are an increasing number of instances, particularly with respect to cybersecurity events or potential data breach, where an affected institutions or its customers might hear of the event through public reporting before being informed by its third party service provider which might have been affected by a disruption. Specialized risk monitoring services can provide particular value to banking organizations in this regard, often through a collaborative or utility offering which is effective and cost-efficient. Significant experience has been gathered in recent years in analogous "negative news" monitoring by external specialists which is relied upon by banks both in connection with anti-money laundering, counter-fraud and broader anti-financial crime ongoing due diligence requirements, as well as in identifying information security risks.

In conclusion, the Proposed Guidance should more clearly emphasize that shared solutions are likely not only to be effective and efficient with respect to "due diligence" (the term used in your questions for comment 14 and 15), but throughout all aspects of the Risk Management Life Cycle (including the additional stage suggested in response to question for comment number 1 above).

*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?*

Consultations with a range of banking organizations and third party service providers has consistently confirmed that identifying and attempting to conduct due diligence on subcontractors with which there is no direct relationship is one of the greatest challenges in applying risk management principles. As noted above, shared solutions could contribute to more efficient and effective due diligence and monitoring in this regard.

The finalization and issuance of the 2021 Incident Notification NPRM together with revisions to the Proposed Guidance can be expected to materially facilitate the efforts of banking organizations to identify and apply appropriate mitigation to subcontractor risks. The reason is that the NPRM in part would apply notification requirements to the third party service providers themselves, substantially raising awareness of the regulatory requirements and their seriousness. Currently, the level of appreciation among third party service providers of the regulatory expectations on banks under the Proposed Guidance (or pre-existing guidance) is inconsistent. It is lower for service providers in the IT area who are not specialized solely to focus on banks. Banking organisations consistently report the delays or lack of responsiveness among some service providers and moreso in seeking to obtain relevant information about subcontractors. Applying the NPRM's specific notification requirements to service providers would effectively move significant aspects of the risk management awareness and focus on step further down the outsourcing chain. The service providers would also be further incentivized to oversee their own reliance on subcontractors (or sub-subcontractors) in order to be able to meet notification requirements directly applicable to them.

With respect to "chain" risks, 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 given third party relationship. Moreover, helping banking institutions--and in turn their supervisors--to better understand chains of subcontractors would help to identify possible concentration risks for an individual institution or for the industry as a whole that would not necessarily be apparent only by observing direct third party service provider relationships. Again, shared solutions could be instrumental in helping to identify such concentration risks.

*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?*

The concepts discussed in the OCC's 2020 FAQs should be incorporated into the Proposed Guidance, and those FAQs should subsequently be withdrawn.

## VI. Final Comments

We hereby incorporate by reference a separate comment letter being filed on the Proposed Guidance by Market Integrity Solutions, LLC, which raises additional issues beyond this submission with which we also agree.

Thank you for the opportunity to comment on the Proposed Guidance, and in particular the importance of finalizing the related NPRM on Incident Notifications. If we may provide further assistance, please feel free to contact us at (202) 990-6990 or info@crindata.com.

Sincerely,

CRINDATA

By: *James H. Freis, Jr.*
James H. Freis, Jr.
Co-Founder & Chairman

*Mark Stetler*
Mark Stetler
Co-Founder & CEO