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