Promontory Interfinancial Network, LLC
1300 North 17th Street
Suite 1800
Arlington, VA 22209-3810

T 703-292-3400
F 703-528-5700

www.promnetwork.com

February 15, 2017

Board of Governors of the Federal Reserve System
regs.comments@federalreserve.gov
Docket No. R–1550 and RIN 7100–AE–61

Office of the Comptroller of the Currency
regs.comments@occ.treas.gov
Docket ID OCC–2016–0016

Federal Deposit Insurance Corporation
comments@fdic.gov
RIN 3064–AE45

Re: Advance Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards

Ladies and Gentlemen:

On behalf of Promontory Interfinancial Network, LLC ("*Promontory Network*"),[1] I write to comment on the Advance Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards issued by the Board of Governors of the Federal Reserve System (the "*Board*"), the Office of the Comptroller of the Currency (the "*OCC*"), and the Federal Deposit Insurance Corporation (the "*FDIC*") on October 26, 2016 (the "*ANPR*").[2]

INTRODUCTION AND SUMMARY

The ANPR acknowledges that "[t]he Board, the OCC, and the FDIC have incorporated information security into their supervisory review of information technology (IT) programs at supervised banking organizations for many years."[3] The ANPR also acknowledges that the agencies already "review the services of third-party service providers that support those entities . . . ."[4] The ANPR does not identify any cybersecurity-related shortcoming in existing supervision. Nor does it show that more regulation would produce better results.

---

[1] Founded in 2002, Promontory Network provides services to the banking and brokerage industries. Promontory Network's deposit allocation and sweep services include CDARS®, the Certificate of Deposit Account Registry Service®, for time deposits, ICS®, the Insured Cash Sweep® service, for non-time deposits, and IND®, the Insured Network Deposits® service, for non-time deposits swept to banks primarily by broker-dealers.

[2] Advance Notice of Proposed Rulemaking on Enhanced Cyber Risk Management Standards, 81 Fed. Reg. 74,315 (October 26, 2016).

[3] *Id.* at 74,316.

[4] *Id.*

Nevertheless, according to the ANPR, "[i]n response to expanding cyber risks, the agencies are considering establishing enhanced standards for the largest and most interconnected entities under their supervision, as well as for services that these entities receive from third parties."[5] The ANPR states: "The enhanced standards would be designed to increase covered entities' operational resilience and reduce the potential impact on the financial system in the event of a failure, cyber-attack, or the failure to implement appropriate cyber risk management."[6]

No one disputes that cybersecurity is enormously important. Banks face large and growing cybersecurity threats and must commit substantial resources to preventing harm. It does not follow, however, that more cybersecurity regulation would mean better cybersecurity. Even if one assumes that, in general, regulation is a good thing, too much of a good thing often causes harm.[7] A rulemaking that imposed overlapping new cybersecurity standards on top of the multiple existing standards, without any empirical analysis of actual effects, would be counterproductive. Rather than improving cybersecurity, such a rulemaking would divert to unproductive compliance processes the very resources that covered entities could otherwise devote to securing operations.[8]

More specifically, Promontory Network comments as follows on the ANPR[9]:

---

[5] *Id.*

[6] *Id.* Because people often understand "enhanced" to mean "improved," referring to the contemplated standards that are described in the ANPR as "enhanced standards" implies that they would be an improvement over existing standards and other alternatives. Whether they actually would be an improvement, however, is one of the central questions posed by the ANPR. That question should not be prejudged by choice of terminology. Therefore, this comment letter refers to the "enhanced standards" more neutrally as the "ANPR standards."

[7] *See* Jason R. Pierce & Herman Aguinis, *The Too-Much-of-a-Good-Thing Effect in Management*, 39 Journal of Management 313, 314 (2013) (describing the management phenomenon of "ordinarily beneficial antecedents causing harm when taken too far").

[8] *See* Eli Dourado & Andrea O'Sullivan, *Poor Federal Cybersecurity Reveals Weakness of Technocratic Approach*, Mercatus Center, George Mason University (June 2015), https://www.mercatus.org/publication/poor-federal-cybersecurity-reveals-weakness-technocratic-approach.

[9] In addition to addressing the enumerated comments, the agencies should clarify that the scope of the ANPR is cybersecurity, not all things cyber, *i.e.*, not everything that in any way involves computers or networks. The ANPR frequently uses the word "cybersecurity," which Merriam-Webster.com defines as "measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack." The ANPR also uses various other cybersecurity-related terms, including "cyber contagion," ANPR at 74,324, "cyber resilience," *id.* at 74,315, 74,317, 74,320, 74,324, 74,325, 74,326, "cyber threat," *id*. at 74,317, 74,322, 74,323, 74,325, "cyber vulnerability," *id.* at 74,318, and "cyber-attack," *id.* at 74,316, 74,317, 74,318, 74,319, 74,320, 74,324, 74,325.

At times, however, the ANPR also uses "cyber" without explicitly limiting it to security. According to Merriam-Webster.com, "cyber" alone means "of, relating to, or involving computers or computer networks (as the Internet)," which in banking today applies to almost everything. In a few instances, the ANPR mentions matters that appear to go beyond cybersecurity, such as when it refers to "opportunities for high-impact technology failures and cyber-attacks." *Id.* at 74,316. The ANPR therefore leaves potentially uncertain the intended meaning of several terms that it

1. The ANPR standards extensively overlap with multiple existing supervisory programs and guidance frameworks.

2. Adopting the overlapping ANPR standards would violate basic principles of sound regulation embodied in Executive Orders issued by Presidents Obama and Trump.

    a. The ANPR fails to identify any shortcoming in existing cybersecurity regulation that would require grafting another layer of standards onto the multiple existing layers.

    b. Even if there were a shortcoming in cybersecurity regulation, the ANPR fails to show that adding another layer of standards would correct it.

    c. Imposing the technocratic ANPR standards on top of existing standards would be more likely to diminish cybersecurity than to enhance it.

    d. Rather than adding a new layer of cybersecurity standards, the agencies should consolidate existing regulatory documents for greater clarity.

3. The need concerning third-party service providers is not for new cybersecurity standards, but for a consistent examination policy.

    a. Even if otherwise adopted, the ANPR standards should not apply to third-party service providers.

    b. Examination practices that subject some service providers to rigorous scrutiny while exempting others are not only unfair, but counterproductive.

---

uses, including "cyber environment," *id.* at 74,326, "cyber event," *id*. at 74,315, 74,319, 74,320, 74,321, 74,322, 74,324, 74,325, "cyber incident," *id.* at 74,316, 74,321, "cyber response," *id.* at 74,325, "cyber risk," *id.* at 74,315-74,326, and "cyber standards," *id.* at 74,315.

Although the context and content of the ANPR standards suggest that the scope is limited to cybersecurity, if the scope instead were broader, the issues with the ANPR that are discussed in this comment letter would be even more extensive. In that case, the agencies should invite further comments to address the broader scope.

DISCUSSION

1. The ANPR standards extensively overlap with multiple existing supervisory programs and guidance frameworks.

The ANPR states that the contemplated rulemaking would not replace, but would be added to, the multiple existing supervisory programs and guidance frameworks for cybersecurity.[10] These supervisory programs include the Uniform Rating System for Information Technology ("*URSIT*"), the Federal Financial Institutions Examination Council ("*FFIEC*") Information Technology Examination Handbook InfoBase ("*FFIEC IT Handbook*"), and the Interagency Guidelines Establishing Information Security Standards (the "*Interagency Guidelines*").[11] The existing supervisory programs are supplemented by multiple non-binding guidance frameworks.[12]

The ANPR standards overlap with the existing programs and frameworks in every one of the ANPR's five categories. For example, in category 1, cyber risk governance, the ANPR standards assign responsibility for information security policy to an entity's board of directors.[13] But the FFIEC IT Handbook already does that, stating: "The board, or designated board committee, should be responsible for overseeing the development, implementation, and maintenance of the institution's information security program and holding senior management accountable for its actions."[14] Using almost identical language, the ANPR redundantly states: "The board of directors of a covered entity would oversee and hold senior management accountable for implementing the entity's cyber risk management framework."[15]

The ANPR also states that the agencies may require the board "to have adequate expertise in cybersecurity or to maintain access to resources or staff with such expertise."[16] The FFIEC IT

---

[10] *Id.* at 74,316-74,317 ("The enhanced standards would be integrated into the existing supervisory framework by establishing enhanced supervisory expectations for the entities and services that potentially pose heightened cyber risk to the safety and soundness of the financial sector.").

[11] *See id.* at 74,317.

[12] *See id.* at 74,317-74,318. These frameworks include the FFIEC Cybersecurity Assessment Tool, the National Institute of Standards and Technology ("*NIST*") Cybersecurity Framework, the Committee on Payments and Market Infrastructures ("*CPMI*") and the Board of the International Organization of Securities Commissions ("*IOSCO*") Guidelines on Cyber Resilience for Financial Market Infrastructures ("*CPMI/ISOCO Guidance*"), and the Board, OCC, and Securities and Exchange Commission ("*SEC*") Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System ("*Sound Practices Paper*"). *See id.*

[13] *See id.* at 74,320-74,322.

[14] FFIEC IT Handbook, Information Security (2016), at I.B., http://ithandbook.ffiec.gov/it-booklets/information-security/i%20governance-of-the-information-security-program/ib%20responsibility-and-accountability.aspx.

[15] ANPR at 74,321.

[16] *Id.*

Handbook states that "the board and management should understand and support information security."[17] The difference, if any, is slight. Whether having "adequate expertise in cybersecurity" (or access to such expertise) differs from "understand[ing] and support[ing] information security," and, if so, how, is anybody's guess.

In category 2, cyber risk management, which itself overlaps with cyber risk governance, the ANPR states that the ANPR standards "would require covered entities, to the greatest extent possible and consistent with their organizational structure, to integrate cyber risk management into the responsibilities of at least three independent functions (such as the three lines of defense risk-management model) with appropriate checks and balances."[18] The FFIEC IT Handbook, however, already calls for management to develop and implement an information security program that "[i]ntegrates with lines of business and support functions."[19] Again, the difference, if any, is slight, leaving covered entities and agency personnel to puzzle over whether, and, if so, how, the overlapping standards are meant to differ.

The same pattern permeates the remainder of the ANPR. The ANPR standards in category 3, internal dependency management, overlap in numerous respects with existing supervisory programs and guidance frameworks,[20] as do the ANPR standards in category 4, external dependency management,[21] and all three components of category 5, incident response, cyber resilience, and situational awareness.[22]

---

[17] FFIEC IT Handbook, Information Security (2016), at I.A, http://ithandbook.ffiec.gov/it-booklets/information-security/i%20governance-of-the-information-security-program/ia%20security-culture.aspx.

[18] ANPR at 74,321.

[19] FFIEC IT Handbook, Information Security (2016), at II, http://ithandbook.ffiec.gov/it-booklets/information-security/ii%20information-security-program-management.aspx.

[20] *Compare*, *e.g.*, ANPR at 74,323 (periodic testing of backups) *with* FFIEC IT Handbook, Business Continuity Planning (2016), Appendix G, http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/appendix-g-business-continuity-plan-components.aspx; ANPR at 74,323 (maintaining an inventory of all business assets on an enterprise-wide basis) *with* FFIEC IT Handbook, Information Security (2016), at II.C.5, *and* FFIEC Cybersecurity Assessment Tool at 22-23, https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_June_2015_PDF2.pdf, *and* NIST Cybersecurity Framework at 22, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf, *and* CPMI/IOSCO Guidance at 3.2.2, http://www.bis.org/cpmi/publ/d146.pdf, *and* Sound Practices Paper, at Sound Practices section, paragraph 1, https://www.sec.gov/news/studies/34-47638.htm.

[21] *Compare*, *e.g.*, ANPR at 74,323-74,324 (establishing controls to address cyber risk presented by each external partner) *with* FFIEC IT Handbook, Management (2016), at III.C.3., http://ithandbook.ffiec.gov/it-booklets/management/iii-it-risk-management/iiic-risk-mitigation/iiic3-information-security.aspx (referencing FFIEC Cybersecurity Assessment Tool for additional information), *and* Interagency Guidelines at VII, *and* Assessment Tool at 50, *and* NIST Framework at 31, *and* CPMI/IOSCO Guidance at 4.3.1.b.

[22] *Compare*, *e.g.*, ANPR at 74,324 (establishing and maintaining effective incident response governance strategies and establishing and maintaining enterprise-wide cyber resilience and incident response programs) *with* FFIEC IT Handbook, Business Continuity Planning (2016), at Other Policies, Standards and Processes, Incident Response *and*

To the extent the ANPR standards are meant to have the same meaning as provisions in existing supervisory programs and guidance frameworks, they are unnecessary. To the extent they are meant to have different meanings, they would cause inconsistency and confusion. In either case, they would require each covered entity, as well as each agency, to waste large amounts of resources on the process of attempting to apply the multiple existing standards, attempting to apply the overlapping but not identically-worded ANPR standards, attempting to understand how, if at all, they differ, and attempting to determine, if they differ, what to do about it.

2. Adopting the overlapping ANPR standards would violate basic principles of sound regulation embodied in Executive Orders issued by Presidents Obama and Trump.

Executive Order 13563, issued in 2011 by President Obama (the "*Obama EO*"),[23] directs agencies to avoid regulatory requirements that are "redundant, inconsistent, or overlapping."[24] The Obama EO also requires that agencies engage in "retrospective analysis" of the actual effects of existing rules so that further rulemaking can take into account those effects.[25] Although the Obama EO does not directly apply to the Board, the OCC, or the FDIC, the agencies have committed themselves to its principles.[26] For example, the OCC has stated that it seeks to improve its

---

Interagency Guidelines at IV; ANPR at 74,325 (proposing a recovery time objective ("*RTO*") of two hours for sector-critical systems) *with* Sound Practices Paper at Sound Practices section, paragraph 2, *and* CPMI/IOSCO Guidance at 6.2.2. An RTO, of course, is an objective, not a certainty, and actual recovery time depends on what is possible in the circumstances, which cannot be fixed by regulation.

[23] Exec. Order No. 13563, 76 Fed. Reg. 3821 (2011), https://www.federalregister.gov/documents/2011/01/21/2011-1385/improving-regulation-and-regulatory-review.

[24] *Id.* § 3.

[25] *Id.* § 6(a).

[26] Letter from R. Bruce Josten, Exec. Vice President, Government Affairs, to Richard Shelby, Chairman, S. Comm. on Banking, Hous., and Urban Affairs, and Sen. Sherrod Brown, S. Comm. on Banking, Hous., and Urban Affairs (June 6, 2016), https://www.uschamber.com/sites/default/files/documents/files/160606_senate_banking_committee_hearing_on_bank_capital_and_liquidity_regulation_shelby_brown.pdf ("the FDIC, Federal Reserve, and the OCC have committed to abide by Executive Order 13563"); Letter from Ben Bernanke, Chairman of the Board of Governors of the Federal Reserve System, to Cass Sunstein, Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget (Nov. 8, 2011), https://www.federalreserve.gov/foia/files/regulatory-burden-reduction-111115.pdf (describing Federal Reserve efforts "to abide by the principles described in . . . Executive Order [13563]"); Letter from John Walsh, Acting Comptroller of the Currency, to Cass Sunstein, Administrator, Office of Information and Regulatory Affairs, Office of Management and Budget (Nov. 29, 2011), https://occ.gov/topics/laws-regulations/increasing-regulatory-effectiveness.pdf (describing OCC efforts to act "consistent with the goals of Executive Order 13563"); Office of Inspector General, Federal Deposit Insurance Corporation, Evaluation of the FDIC's Economic Analysis of Three Rulemakings to Implement Provisions of the Dodd-Frank Act, Report No. EVAL-11-003, at 3 (June 2011) (referring to the FDIC addressing "spirit" and "principles" of Executive Order 13563).

regulations "to make them more effective by combining them where possible, reducing duplication, and eliminating unnecessary requirements."[27]

The ANPR takes the opposite approach. Rather than combining the multiple existing sets of cybersecurity standards to reduce the overlap that already exists, the ANPR proposes – with no retrospective analysis of the effects of existing standards – to add yet another overlapping layer of cybersecurity standards. This approach is at odds with the principles of the Obama EO.

Executive Order 13771, issued in 2017 by President Trump (the "*Trump EO*"),[28] states that "it is important that for every one new regulation issued, at least two prior regulations be identified for elimination . . . ."[29] The Trump EO also provides that, for the current fiscal year and subject to exceptions not pertinent here, "the total incremental cost of all new regulations, including repealed regulations, to be finalized this year shall be no greater than zero, unless otherwise required by law" or consistent with advice from the OMB director.[30] Although the Trump EO, like the Obama EO, does not directly apply to the Board, the OCC, or the FDIC, we assume that the agencies, consistent with past practice, intend to adhere to its principles.

The ANPR proposes to add a new set of regulations without identifying any regulations for elimination. By adding such new regulations, the ANPR would impose a net cost well above zero. The ANPR therefore is inconsistent with the principles of sound regulation described in the Trump EO as well as the Obama EO.

a. The ANPR fails to identify any shortcoming in existing cybersecurity regulation that would require grafting another layer of standards onto the multiple existing layers.

Professor Cass R. Sunstein of Harvard Law School served as Administrator of the Office of Information and Regulatory Affairs from 2009 to 2012, with responsibilities encompassing the Obama EO. In describing the retrospective analysis required by the Obama EO, Professor Sunstein points out that, for a regulatory system to be sensible, the question whether to expand rules must be considered "in light of what we learn about <u>what those rules are actually doing</u>."[31] He observes:

---

[27] Letter from John Walsh, Acting Comptroller of the Currency, *supra* note 26.

[28] Exec. Order No. 13771, Presidential Executive Order on Reducing Regulation and Controlling Regulatory Costs, 82 Fed. Reg. 9339 (2017), https://www.federalregister.gov/documents/2017/02/03/2017-02451/reducing-regulation-and-controlling-regulatory-costs.

[29] *Id.* § 1.

[30] *Id.* § 2(b).

[31] Cass R. Sunstein, *Symposium: Keynote Address: The Regulatory Lookback*, 94 B.U.L.REV. 579, 580 (2014) (emphasis added).

> It is an astonishing fact that until very recently, there has been no sustained effort to gather, let alone act on, that information – and that existing efforts remain highly preliminary and partial. Such an effort might well help agencies to simplify the system by eliminating unjustified burdens and a great deal of pointless red tape.[32]

The ANPR makes no effort to gather, let alone to act on, any information about what the existing standards are actually doing. As a result, it cannot, and does not, provide any evidence that another layer of cybersecurity standards is needed or would add anything but more of what Sunstein calls "pointless red tape."

The ANPR merely states that financial institutions and consumers "have become increasingly dependent on technology to facilitate financial transactions" and that "the largest, most complex financial institutions rely heavily on technology . . . ."[33] This vague statement could have been made with equal force for well over a decade. It does not state any fact that suddenly warrants a major new rulemaking in 2017.

The ANPR also asserts that "cyber risk has the potential to produce losses large enough to threaten an entity's financial health, its reputation, or its ability to maintain core operations if faced with a material cyber event."[34] If true, this fact is also not new. The ANPR does not, however, cite a single case, and to Promontory Network's knowledge there is no case, in which a bank has failed because of a "cyber event," much less a case in which some deficiency in existing cybersecurity regulation was responsible for a failure.

On the contrary, in 2011, the Office of Inspector General of the Board provided a report to Congress presenting a Summary Analysis of Failed Bank Reviews.[35] The report described as the "common themes" in failures (1) poor management decisions on growth and strategic choices, (2) excessively rapid loan growth, (3) excessive asset concentrations in commercial real estate or construction, land, and land development loans, and (4) insufficient capital.[36] None of these themes has anything to do with cybersecurity or any failure of cybersecurity regulation.

b. Even if there were a shortcoming in cybersecurity regulation, the ANPR fails to show that adding another layer of standards would correct it.

Even if there were shown to be a shortcoming in existing cybersecurity regulation, it would not warrant simply assuming that adding another layer of standards would make things better.

---

[32] *Id.*

[33] ANPR at 74,316.

[34] *Id.* at 74,321.

[35] Office of Inspector General, Board of Governors of the Federal Reserve System, Summary Analysis of Failed Bank Reviews (2011), https://oig.federalreserve.gov/reports/Cross_Cutting_Final_Report_9-30-11.pdf.

[36] *Id.* at 8.

There would also have to be a showing that the ANPR standards would actually improve cybersecurity. That showing, in turn, would require some empirical evidence or other sound basis to believe that, other things being equal, entities that act as the ANPR standards prescribe are less likely than other entities to experience serious cybersecurity problems. The ANPR merely assumes without evidence that the ANPR standards will improve cybersecurity and asks no questions that would help elicit such evidence if it existed.

Rather than showing that the ANPR standards would reduce cybersecurity risk, the ANPR acknowledges that "the agencies are not aware of any consistent methodologies to measure cyber risk across the financial sector using specific cyber risk management objectives."[37] It states that the agencies are "seeking to develop," but have not yet developed, "a consistent, repeatable methodology to support the ongoing measurement of cyber risk within covered entities."[38]

Lacking any methodology to measure cyber risk, the agencies cannot have measured existing cyber risk or compared it with cyber risk under alternative approaches to cybersecurity. As a result, they cannot have reached any evidence-based or data-driven determination that the proposed new layer of cybersecurity standards would reduce risk at all, or even that it would not make risk worse. To impose a new layer of cybersecurity standards before being able to measure cybersecurity risk would be to put the cart miles before the horse.

c. Imposing the technocratic ANPR standards on top of existing standards would be more likely to diminish cybersecurity than to enhance it.

The ANPR reflects a pattern described by Eli Dourado and Andrea O'Sullivan of George Mason University:

> Sweeping technocratic solutions are iteratively imposed every few years with little-to-no understanding or continuity with previous policies. Abstract consistencies in top-down planning break down on the human level as personnel struggle to make sense of redundancies and eventually ignore complex reporting and procedural standards. Fundamental issues of talent recruitment and personnel training go relatively unaddressed as offices struggle to keep up with the changing security checklists, which may or may not actually translate to good cybersecurity outcomes.[39]

The process of which the ANPR is a part bears an uncanny resemblance to this description. If adopted, new regulations with the ANPR standards would be the latest of multiple "[s]weeping technocratic solutions" for cybersecurity that are "imposed every few years." The imposition

---

[37] ANPR at 74,326.

[38] *Id.*

[39] Eli Dourado & Andrea O'Sullivan, *supra* note 8.

would occur with no assessment of previous policies or their effectiveness and with no evidence that the ANPR standards would "actually translate to good cybersecurity outcomes." Because the ANPR standards extensively overlap with existing standards, they would introduce redundancies, which personnel would "struggle to make sense of." The ANPR standards would also take resources away from substantive matters, such as recruitment, training, and operations, as entities "struggle[d] to keep up with the changing security checklists."

As these effects show, imposing the ANPR standards would be likely to make matters not better, but worse. The ANPR standards consist primarily of paperwork-oriented requirements, such as requirements for "policies, procedures, practices, controls, personnel and systems" in each of the five categories,[40] rather than substantive requirements, such as encryption or two-factor authentication. Compliance with the requirements would require more personnel across the board. Dividing cybersecurity tasks among more persons, pursuant to more regulations, only complicates the effort. Covered entities do not have unlimited resources. Increasing an entity's bureaucratic burden diverts its limited resources from more productive uses, including operational functions that are essential to safety and soundness.

d. Rather than adding a new layer of cybersecurity standards, the agencies should consolidate existing regulatory documents for greater clarity.

Consistent with the principles of the Executive Orders cited above and the stated intent of the OCC to make its regulations "more effective by combining them where possible" and "reducing duplication,"[41] the agencies should consolidate the existing layers of cybersecurity standards, rather than adding to them and thereby introducing more duplication.

The agencies, in consolidating existing layers of cybersecurity standards, should use existing flexible guidance rather than rigid, one-size-fits-all rules. Flexible guidance empowers examiners to use their expertise to avoid nonsensical or harmful results. Rigid rules have the opposite effect. As the ANPR makes clear, the agencies acknowledge that each covered entity is entitled to pursue its own "risk appetite and strategy" and its own "cyber risk tolerances."[42] It would be anomalous, having allowed entities the flexibility to set their own risk appetite, strategy, and tolerances – reflecting their own goals – to deny them flexibility in determining how best to pursue those goals.

---

[40] ANPR at 74,326.

[41] Letter from John Walsh, Acting Comptroller of the Currency, *supra* note 26.

[42] ANPR, at 74,321.

3. The need concerning third-party service providers is not for new cybersecurity standards, but for a consistent examination policy.

Under the Bank Service Company Act, when a third party performs certain types of services – such as check and deposit sorting and posting, computation and posting of credits and charges, and the like – for a federally regulated bank, the performance of the services is subject to regulation and examination by a federal banking agency as if the services were being performed by the bank itself.[43] As with other potentially covered entities, however, the ANPR provides no basis to conclude that existing standards are insufficient. In the case of third-party service providers, the problem is not with the regulatory tools, but with their arbitrarily selective use.

a. Even if otherwise adopted, the ANPR standards should not apply to third-party service providers.

Even if the ANPR standards are adopted for banking organizations, they should not apply to third-party service providers. Among other things, applying the ANPR standards to third-party service providers would impose unwarranted costs on all types of banking organizations, including community banks, and would undermine the uniformity of the Uniform Rating System for Information Technology.

The ANPR states that "the agencies are considering establishing a two-tiered approach, with the enhanced standards applying to all systems of covered entities, and an additional, higher set of expectations, referred to in the ANPR as 'sector-critical standards,' applying to those systems of covered entities that are critical to the financial sector."[44] More broadly, the ANPR describes three tiers, with existing standards for non-covered entities (*low tier*), existing standards plus general ANPR standards for covered entities (*middle tier*), and existing standards plus general ANPR standards plus "sector-critical" ANPR standards for sector-critical entities (*high tier*).

If, as the ANPR appears to contemplate, a service provider would be subjected to the ANPR standards on the basis of the tiers occupied by the entities it served,[45] and if it served entities in more than one tier, the service provider would become subject to multiple different sets of standards. Given the nature of the ANPR standards, many of which apply to company-wide or business unit-wide procedures, a provider would often effectively be required to comply, across the board, with the most stringent standards, even though many or most of the provider's customers

---

[43] 12 U.S.C. §§ 1863, 1867(c)(1). The regulatory authority is limited to the performance of specified types of services and does not extend to plenary regulation of the provider by the federal banking agencies. The bank remains responsible for the services performed by the third party.

[44] ANPR at 74,319.

[45] *See id.* at 74,318.

were community banks.[46] The result would be to raise costs for all customers, including community banks.[47]

By excluding third-party service providers from the scope of the ANPR standards, the agencies could avoid this result and use more flexible standards to promote risk-based measures that were commensurate with the makeup of the customer base and the nature of the services provided.[48] The provider's community bank customers could then be spared from having to pay for the provider's compliance with standards that did not apply to them.

A further reason to exclude third-party service providers from the scope of the ANPR standards is that including them could undermine the uniformity of the Uniform Rating System for Information Technology. The ANPR acknowledges that both federal and state regulators use the URSIT rating "to uniformly assess IT risks" at all types of financial institutions, including community banks, and at service providers to all types of financial institutions, including service providers to community banks.[49] The ANPR also states that "[t]he proposed enhanced standards would not replace the URSIT ratings but could be used, in part, to inform the cyber-related elements of the URSIT rating for covered entities."[50]

If the ANPR standards "inform[ed]" the URSIT rating for service providers that performed services for covered entities, but not for service providers that performed services only for non-covered entities, regulators could no longer use the URSIT rating "to uniformly assess IT risks," because providers of the same services would be rated on the basis of different standards. For example, if one service provider performed services for a covered entity, and another service provider performed identical services for a non-covered entity, the two service providers could receive different URSIT ratings not because of any difference in the performance of services, but

---

[46] A banking organization in most cases is likely to occupy only one of the three tiers and therefore to be subject only to the standards that correspond to that particular tier. Third-party service providers, however, often provide services to entities in more than one tier.

[47] For example, if the same provider system served customers at all tiers, a system RTO of two hours for one high-tier customer would entail the same RTO for all customers, and special procedures triggered by one high tier customer would be required even though not triggered by other customers. If the provider had 100 community bank (low tier) customers, 10 non-critical large bank (middle tier) customers, and only one sector-critical large bank (high tier) customer, the 100 community bank customers and 10 non-critical large bank customers would be paying for the provider's compliance with elevated standards that did not apply to them.

[48] In the example above, the primary users of the provider's services, by far, are community banks. Given this fact, the services, even when provided to a single sector-critical large bank, are likely to relate to a small portion of that bank's overall business that is not sector-critical.

[49] ANPR at 74,317.

[50] *Id.*

because different standards applied to the same services. The uniformity of URSIT ratings, as a result, would be impaired.

b. Examination practices that subject some service providers to rigorous scrutiny while exempting others are not only unfair, but counterproductive.

The need is not for a new regulation of third-party service providers, but for an end to arbitrarily selective examination of third-party service providers. Promontory Network's own experience illustrates this point. Since 2010, Promontory Network has undergone three full multi-week technology service provider examinations and two multi-week technology service provider visitations led by the FDIC. To the best of Promontory Network's knowledge, however, none of the other entities that provide technology services similar to Promontory Network's services has undergone even one examination or visitation.[51]

The performance of services similar to Promontory Network's by other entities is no less within the scope of the Bank Service Company Act, and by any measure, the amounts of depositor funds that the other entities process are material. The other entities include service providers that have publicly claimed to process balances of more than $1.7 billion, more than $8 billion, more than $16 billion, and more than $30 billion. Nevertheless, the agencies have effectively exempted all the other entities from the rigorous scrutiny that is applied to Promontory Network. Although Promontory Network places the highest priority on cybersecurity and welcomes appropriate scrutiny, the exemption of other providers from the same scrutiny is unwarranted.

Consistent application of standards requires that, if one service provider is examined, all be examined. Selective examination of one provider, with all others exempted, inappropriately places the examined provider at a competitive disadvantage. In doing so, it may give rise to the inference, whether or not warranted, that examination is being used to target a particular provider for extraneous reasons. If it appears that regulatory authority is being deployed differently for favored and disfavored providers, confidence in the process is diminished, and some providers may focus more on trying to become favored than on trying to fulfill regulatory expectations.

In addition, selective examination that arbitrarily exempts all but one service provider causes broader negative effects. For example, being examined consumes substantial resources, not only in the substantial attention required from numerous company personnel during the examination, but also in ongoing activities and procedures prompted by examination findings. If only one service provider incurs these costs, the unexamined providers have lower costs. Having lower costs, they are able to offer their customers lower prices than they otherwise could. If the examined provider offers better cybersecurity, selective examination that enables the lower-cost unexamined providers to attract more customers reduces cybersecurity overall.

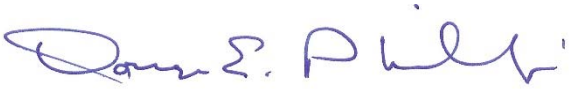
---

[51] Promontory Network understands that one or two such entities may have undergone a discovery review, which Promontory Network has also undergone, but nothing further.

* * *

Thank you for consideration of our comments. Should you wish to discuss them further, please contact the undersigned at (703) 292-3338 (dphillips@promnetwork.com).

Sincerely,



Douglas E. Phillips
Senior Vice President and General Counsel