TSYS®

General Counsel's Office
One TSYS Way
Post Office Box 2567
Columbus GA 31902-2567

+1.706.644.0199 tel

February 17, 2017

By Electronic Delivery to regs.comments@federalreserve.gov, regs.comments@occ.treas.gov and Comments@fdic.gov

Robert deV. Frierson, Secretary,
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Washington, DC 20551

Legislative and Regulatory Activities Division
Office of the Comptroller of the Currency
400 7th Street SW., Suite 3E–218
Washington, DC 20219

Robert E. Feldman, Executive Secretary
Attention: Comments
Federal Deposit Insurance Corporation
550 17th Street NW
Washington, DC 20429

RE: FRB – Docket No. R–1550 and RIN 7100–AE–61
OCC – Docket ID OCC–2016–0016'
FDIC – RIN 3064–AE45

This letter is submitted by Total System Service, Inc. ("TSYS") in response to the joint advance notice of proposed rulemaking ("ANPR") by the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation ("Agencies") to establish enhanced cyber risk management standards for certain large and interconnected financial institutions. 81 Fed. Reg. 74,315 (Oct. 26, 2016).

TSYS appreciates the opportunity to comment on the ANPR and the important issue of cybersecurity. In particular, TSYS wishes to comment on the potential application of enhanced cyber standards to third parties that provide services to covered financial institutions. In addition, TSYS also supports the comments submitted by the Financial Services Roundtable and the Electronic Transactions Association on the ANPR.

TSYS commends the Agencies for their consideration of the potential impact on the U.S. financial system of a significant cybersecurity incident impacting a large and interconnected financial institution. Few issues are more important in today's environment in which cybersecurity threats are growing both in complexity and volume. Nonetheless, as the Agencies know, this is a very complex issue, and there are substantial challenges in creating a workable standard that enhances cybersecurity protections at critical financial institutions in a meaningful way, without creating unintended negative consequences. While theoretically significant, the impact on the safety and soundness of the financial system of a significant cyber event at a large and interconnected financial institution is in fact unknown. It is difficult, if not impossible, to create a single standard that elevates the level of cybersecurity protection at critical financial institutions in a way that is balanced against the actual risks and the likelihood that those risks will be realized.

Issues of scope are particularly relevant to consideration of the potential costs and benefits associated with enhanced cyber standards, as well as the likelihood that those costs and benefits can be accurately quantified and realized. For example, in order to protect the financial system, should the Agencies impose enhanced standards that apply to all systems and operations of covered financial institutions, or only those systems that could have a significant impact on the financial institution or the financial system? Are the benefits of applying the enhanced standard on an enterprise-wide basis to the numerous affiliates and subsidiaries of the few financial institutions that would be directly covered outweighed by the significant burden that would result and the fact that those affiliates and subsidiaries likely do not present the same risks (if any) to the financial system? Should the enhanced standards be applied to all third-party service providers to covered financial institutions equally? At this time, there are more questions than answers, as highlighted by the Agencies' own inquiry. As a result, the Agencies are to be commended for raising these issues in the form of the ANPR and soliciting feedback, as opposed to proposing a more formal proposed rule.

The Agencies Should Not Impose Enhanced Standards on Third-Party Service Providers

We believe that the Agencies should not apply, whether directly or indirectly, any enhanced standards on third-party service providers, for various reasons highlighted in this letter. Instead, we believe that the Agencies should allow covered financial institutions to continue to manage their third-party service provider relationships as contemplated under various guidance issued by the Agencies. In the context of existing requirements and consistent with the Bank Service Company Act and third-party risk management guidance, the Agencies consistently reiterate that the use of a third-party service provider does not relieve a financial institution of its obligation to comply with applicable requirements. *See, e.g.*, OCC Bulletin 2013-29 (Oct. 30, 2013), *available at* https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html (providing that "[a] bank's use of third parties does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in a safe and sound manner and in compliance with applicable laws"). This is a known and understood approach under which both financial institutions and third-party service providers have significant experience operating. Under this approach, a covered financial institution would still be responsible for compliance with any enhanced standards, including to the extent that a third-

party service provider relationship implicates or impacts that compliance. This approach, however, would provide covered financial institutions with the appropriate flexibility to manage their relationships in a risk-based manner taking into account and distinguishing between the wide spectrum of risks relevant to those relationships.

While the clear focus of the Agencies is the enhancement of cybersecurity at the financial institutional level, we believe that a greater risk to the financial sector lies in the threat of a regional interdiction (*e.g.*, sabotage or nation state attack) of the power and telephony grids on which the financial sector relies. As a result, we would encourage the Agencies to continue to work with the Department of Homeland Security to assess the regional impact on the financial sector in the event that the power and telephony grids are impacted by a cyber event.

Although we believe that the Agencies should not apply enhanced standards to third-party service providers under either a direct or indirect approach, we provide the following comments regarding the challenges associated with attempting to do so.

Questions Regarding Third-Party Service Providers

While the ANPR questions how enhanced standards could be effectively applied to critical financial institutions, we believe that the most difficult aspect of any proposal will be the potential application of such standards to third-party service providers. In this regard, the Agencies highlight in the ANPR that they are "considering whether to apply the standards to third-party service providers with respect to services provided to" covered financial institutions, referred to in the ANPR as the "covered services." 81 Fed. Reg. at 74,318. The Agencies believe that some application of enhanced standards to third-party service providers would "ensure consistent, direct application of the standards regardless of whether a" covered financial institution or its third-party service provider performed the service. *Id.* To address this issue, the Agencies appear to be considering two distinct approaches: (1) applying the enhanced standards directly to third-party service providers; or (2) requiring that covered financial institutions "flow down" their obligations under the enhanced standards to their third-party service providers.

Service Provider Definition

While the ANPR signals potential application to third-party service providers, the ANPR jumps immediately to questions of how to apply enhanced standards to service providers. The ANPR does not address the difficult issue of scope and specifically how a service provider would be defined (*i.e.*, which service providers would be covered, and whether directly or indirectly). If the only standard for triggering application is whether a company provides services to a covered financial institution, the proposal would potentially apply to tens of thousands of service providers. While the standards considered in the ANPR would apply only to a small number of financial institutions, it is not uncommon for a financial institution to have vendor relationships with hundreds if not thousands of service providers. If the standards are applied on an enterprise-wide basis to the affiliates and subsidiaries of all covered financial institutions, the number of implicated service providers would be exponentially multiplied. Moreover, if the enhanced standards are applied not only to a service provider to a covered

financial institution, but also to other third parties that provide services to the service provider, the scope of application of any rule issued by the Agencies would be dramatic.

As a result, the most important first steps for the Agencies is to define the types or nature of services that would cause a third party to be considered a service provider for purposes of any cyber risk rule. In this regard, financial institutions receive a dramatically wide array of services from third parties, including, for example, food, facility and janitorial services, legal and accounting advice, marketing-related services, lock box services, courier services, cloud and other storage services, transaction processing and backoffice services. There is a spectrum of risk and sensitivity presented by the diverse nature of service provider relationships, and where any given relationship falls on the risk spectrum depends on the exact nature of the service being provided. In order to ensure a workable standard that accomplishes the Agencies' objectives without having an unduly burdensome impact on covered financial institutions and their third-party relationships, the Agencies should ensure that any application of enhanced standards to third-party service providers is risk based, taking into account the risks to the financial system resulting from those relationships. For example, it would significantly impede the ability of a covered financial institution to do business if it had to impose the same security requirements on the food vendor that it imposes on the service provider providing backoffice services that include broad access to customer information and company systems.

The task of defining the types of services or third-party service providers subject to enhanced standards is quite complex, even when approaching the issue in a risk-based manner. For example, the Gramm-Leach-Bliley Act definition of a "service provider" is focused on third parties that are permitted access to customer information and customer information systems in connection with providing services. *See, e.g.*, 12 C.F.R. pt. 30, App. B (OCC). While this definition is risk-based in the sense that it focuses on customer information, numerous service providers, even those presenting minimal risk to a financial institution, would be covered under such a definition, including, for example, service providers that receive limited customer contact information (*e.g.*, e-mail addresses) in connection with providing services (*e.g.*, e-mail vendors). In this regard, the appropriate risks to be considered in this context are risks to the financial system from a significant cybersecurity incident at a critical financial institution. Nonetheless, it will be difficult to address this scope issue in a targeted manner without resulting in broad application even where risk may not warrant coverage. This is particularly true if the Agencies apply the enhanced standards on an enterprise-wide basis to all affiliates and subsidiaries of a covered financial institution.

Levelling the Playing Field for Both Covered Financial Institutions and Service Providers With Respect to Service Relationships

In considering third-party service provider issues, it is also important for the Agencies to take into consideration potential unintended consequences of any requirement for enhanced standards, particularly as it relates to competitive advantages and disadvantages among service providers. For example, if all companies providing services to a covered financial institution were subject to enhanced standards (regardless of risk), it is likely that many of those companies would be forced to terminate their service relationships in order to avoid being subject to a

heightened and rigorous regulatory regime that is not commensurate with the risks and that would eliminate a sustainable profit margin. That is, if the Agencies do not narrowly tailor the service provider aspects of a rule, covered financial institutions may have significant difficulty establishing and maintaining service provider relationships. This would put covered financial institutions at a significant competitive and financial disadvantage to their competitors. For example, covered financial institutions may have to bring many services in-house even if such a move would not be efficient or cost effective. Such a result could in fact create greater risk for covered financial institutions, as established service relationships and the underlying services are put into a state of flux and uncertainty or simply terminated, resulting in need to put in place new processes, infrastructure and personnel in order to perform the functions previously outsourced.

It is also important for the Agencies to consider these same issues from the perspective of third-party service providers. That is, the Agencies should ensure a level playing field, and ensure that the application of enhanced standards to certain service providers does not put those companies at a competitive disadvantage to other service providers and their non-bank and FinTech competitors. For example, if the Agencies conclude that the payments environment and ecosystem presents heightened risk and there is a need to ensure that companies providing services to covered financial institutions in this space are subject to enhanced standards, the Agencies should ensure that all similarly situated participants are subject to the same standards.

Direct v. Indirect Application to Service Providers

In the ANPR, the Agencies question the best way to apply enhanced standards to third-party service providers. As noted above, the Agencies appear to be considering two distinct approaches: (1) applying the enhanced standards directly to third-party service providers; or (2) requiring that covered financial institutions "flow down" their obligations under the enhanced standards to their service providers. As also noted above, we believe that the Agencies should not apply, whether directly or indirectly, any enhanced standards on third-party service providers

If, however, the Agencies seek to impose enhanced standards on third-party service providers, we believe that the second option, an "indirect" approach, is most appropriate. Attempting to apply enhanced standards directly to third-party service providers likely would raise issues regarding the legal authority of the Agencies to do so. For example, it is not clear that the Agencies have statutory authority to impose (let alone enforce) regulatory requirements on the diverse types of non-financial companies that act as third-party service providers to financial institutions, including Internet service providers, common carriers and power companies, notwithstanding the fact that threats (*e.g.*, nation state attacks and sabotage) to these types of entities may create significant risk for the financial sector.

Also, the issue of which third-party service providers would be relevant to the issue of the Agencies' legal authority. That is, the broader the Agencies define a third-party service provider, the issue of legal authority will be increasingly important. In this regard, regulations that raise questions of legal authority would not only create uncertainty, but also create challenges for covered financial institutions in managing third-party relationships where third

parties dispute whether the Agencies have the authority to seek to impose enhanced standards on a third party.

Application to Covered Services Only

To the extent that the Agencies seek to impose enhanced standards on third-party service providers, whether directly or indirectly, the Agencies should ensure that any requirements apply to a third-party service provider only with respect to the covered services provided to a covered financial institution. In this regard, companies that provide services to covered financial institutions (regardless of the scope of covered services or covered financial institutions) also provide services to companies that are not financial institutions, as well as to financial institutions that would not be subject to enhanced standards. That is, all third-party service providers that may be subject to enhanced standards would also provide services, and have other activities, that should be outside the scope of any enhanced standards. In this regard, we believe that there is no justification to seek to impose an enterprise-wide like requirement on third-party service providers that would apply enhanced standards to covered services provided to both covered financial institutions and services provided to all other companies. We believe to do so would create significant disincentives for companies to provide services to financial institutions and would be inappropriate, unduly and overly burdensome to service providers, without providing any meaningful additional security benefits to covered financial institutions.

This point cannot be overstated. If the result of providing services to a covered financial institution would be to cause the company to be subject to enhanced standards even with respect to services provided to other companies, many service providers would simply not agree to continue their relationships with covered financial institutions. As noted above, such a result could in fact create greater risk for covered financial institutions, as established service relationships and the underlying services are put into a state of flux and uncertainty or simply terminated.

Which Standard(s)?

Assuming some application of enhanced standards or potentially sector-critical standards to third-party service providers, there still is the question of which standards. Would the same standards that apply to covered financial institutions apply to their third-party service providers? Or would the Agencies create a set of distinct standards that would apply to service providers specifically? And how would the standards fit within the dizzying array of security requirements to which service providers are subject as a result of their service relationships?

While such questions may appear innocuous, they are in fact difficult questions. For example, would the Agencies take a GLBA-like approach and require that service providers implement "appropriate" safeguards to meet the "objectives" of the standards? *See, e.g.*, 12 C.F.R. pt. 30, App. B (OCC). Or would the Agencies instead require that a third-party service provider meet each standard as if the third-party was itself a covered financial institution?

While the enhanced standards are largely focused on process, governance and strategy, the contemplated standards are both detailed and prescriptive. It is far from clear that it would be appropriate for the Agencies to require third-party service providers to put in place "standards generally expected for large, complex financial institutions" and whether such an approach would even achieve the Agencies' objectives. 81 Fed. Reg. at 74,320. The impact of applying the enhanced standards on third-party service providers would require companies (many of whom may not even be financial institutions) to restructure their boards of directors, change how the boards of directors oversee their companies, create new roles *(e.g.,* a Chief Risk Officer), processes and management strategies and even take steps to reduce risk to the financial sector. Because of the focus on process and putting in place a level of risk management appropriate for "large, complex financial institutions," the enhanced standards would not translate to a third-party service provider and should not impose the same requirements on the third-party service provider as those imposed on the financial institution. Third-party service providers are not in a position to analyze and manage risk to the financial sector.

Because of the clear focus on process, governance and strategy, it is not clear how covered financial institutions would translate the standards in a meaningful way in order to "flow down" those requirements to their third-party service providers. In this regard, without clear guidance from the Agencies, it is likely that covered financial institutions would seek to require that third-party service providers comply with the same standards as the financial institution. More specifically, if it is not clear how a covered financial institution could establish its compliance with respect to third-party service providers, the financial institution likely would seek to require that a third-party service provider comply with each of the enhanced standards. It is critical that the Agencies address this issue clearly in any resulting cyber rule.

Although the sector-critical standards are less focused on process and are more technical in nature, the sector-critical standards raise their own issues. For example, the Agencies indicate that they are considering requiring the implementation of "the most effective, commercially available controls" for sector-critical systems. *Id.* at 74,325. Such a standard would be entirely subjective. The term "system" is not defined. For example, a "system" could include all of the technical infrastructure supporting a process *(e.g.,* the server, the operating system, the firewall, the access controls, the applications running on the server, among other things). If defined broadly, the ambiguity and subjectivity of "most effective, commercially available" could extend to literally thousands of "controls." In order to provide a workable standard (and not to say a flexible standard), the Agencies would have to specify the control(s) that would be considered "most effective." However, this would have the unintended consequence of defining for adversaries and attackers the specific controls that need to be defeated in order to compromise the system.

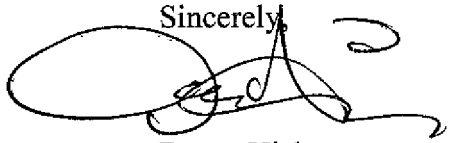
The Agencies are also considering requiring a recovery time objective ("RTO") of two hours for sector-critical systems. *Id.* If covered financial institutions are required to "flow down" this RTO to relevant third-party service providers, covered financial institution likely would have to restructure, renegotiate or simply terminate numerous service agreements and SLAs. In this regard, an RTO of two hours is far from the industry norm or even approaching the typical average seen in the industry. As a result, this would raise significant questions of

financial burden, fairness and competition for third-party service providers. In this regard, the RTO is a critical factor driving pricing in service relationships, and is always a risk-based decision. If a two-hour RTO is a requirement under the sector-critical standard, however, would a third-party service provider be able to charge market rates for such an RTO? Or would this be viewed as a legal requirement on the service provider, the costs of which could not be recouped? It goes without saying that such a result would put third-party service providers at a financial and competitive disadvantage, or could cause such service providers to cease doing business with covered financial institutions.

* * * *

Thank you for the opportunity to comment.

Sincerely,



Deron Hicks
Associate General Counsel
TSYS