MasterCard Worldwide
Law Department
2000 Purchase Street
Purchase, NY 10577-2509

tel 1-914-249-2000
www.mastercard.com

MasterCard Worldwide

January 17, 2017

*Via www.regulations.gov*

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

Legislative and Regulatory Activities Division
Office of the Comptroller of the Currency
400 7th Street, S.W., Suite 3E-218, Mail Stop 9W-11
Washington, DC 20219

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

**RE: Enhanced Cyber Risk Management Standards**
**Federal Reserve System Docket No. R-1550 and RIN 7100-AE-61**
**OCC Docket ID OCC-2016-0016 and RIN 1557-AE06**
**FDIC RIN 3064-AE45**

Dear Sirs and Madams:

Mastercard International Incorporated ("Mastercard") submits this comment letter to 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" and, together with the Board and the OCC, the "Agencies") in response to their request for public comment on the joint advance notice of proposed rulemaking regarding enhanced cyber risk management standards (the "ANPR").[1]

[1] 81 *Fed. Reg.* 74,315 (Oct. 26, 2016).

Mastercard appreciates the opportunity to provide input on the ANPR. Mastercard supports the Agencies' efforts to strengthen cybersecurity within the financial system. However, as discussed below, we encourage the Agencies to reconsider their proposed approach to third-party service providers such as Mastercard under the ANPR.

***Background on Mastercard***

Mastercard is a technology company in the global payments industry. We operate the world's fastest payments processing network, connecting consumers, financial institutions, merchants, governments and businesses in more than 210 countries and territories. Mastercard's products and solutions make everyday commerce activities—such as shopping, traveling, running a business and managing finances—easier, more secure and more efficient for everyone.

Mastercard does not issue credit cards or other payment cards of any type, nor does it contract with merchants to accept those cards. In the Mastercard payment system, those functions are performed in the United States by numerous depository institutions. Mastercard refers to the depository institutions that issue payment cards bearing the Mastercard brands as "issuers." Mastercard refers to the depository institutions that enter into contracts with merchants to accept Mastercard-branded payment cards as "acquirers." Mastercard owns the Mastercard family of brands and licenses depository institutions in the United States to use those brands in conducting payment transactions. Mastercard also provides the networks through which its customer depository institutions can interact to complete payment transactions and sets certain rules regarding those interactions.

When a cardholder presents a Mastercard-branded payment card to a merchant to purchase goods or services, the merchant sends an authorization request to its acquirer, the acquirer routes the request to Mastercard, and Mastercard routes the request to the issuer. The issuer either approves or declines the authorization request and routes its decision back to the merchant through the same channels. Mastercard's role in the transaction is to facilitate the payment instructions between the parties to the transaction—the cardholder, the merchant, the acquirer, and the issuer. In an automated teller machine ("ATM") transaction, Mastercard similarly transmits instructions between the ATM operator and the issuer.

***Mastercard Commitment***

Mastercard invests heavily in the security of the Mastercard system. Over the years, Mastercard has increased dedicated resources to support innovation and technology designed to protect the payments system for cardholders, merchants, and customer financial institutions. Further, our President and Chief Executive Officer, Ajay Banga, served on President Obama's Commission on Enhancing National Cybersecurity (the "Commission"). The Commission provided a report to the President in December 2016 with recommendations for securing and growing the digital economy by strengthening cybersecurity in the public and private sectors. Prior to the formation of the Commission, in 2015, we unveiled plans to invest resources in cybersecurity-related technology enhancements to deliver greater peace of mind for cardholders, merchants and customer financial institutions. These included our 2015 launch of Mastercard Safety Net in the United States, a solution designed to reduce the risk of fraud or cyber attacks before issuers and processors become aware of the threat. Mastercard Safety Net provides an

independent layer of security on top of the tools and policies of financial institutions, by monitoring and blocking specific transactions based on selected criteria.

***Comments on the ANPR***

## *A. Applicability to Third-Party Service Providers*

### 1. Proposed Scope

In the ANPR, the Agencies indicate that they are considering applying the proposed enhanced cyber risk management standards (the "Standards") to U.S. depository institutions, U.S. depository institution holding companies, and U.S. operations or branches of foreign banks with total consolidated assets of $50 billion or more on an enterprise-wide basis (collectively, "covered entities")[2] and their third-party service providers. The Agencies refer to covered entities as the "***largest*** and ***most interconnected*** entities under their supervision."[3]

There are important differences between the banking institutions that would be subject to the Standards under the ANPR and their third-party service providers in terms of size, interconnectedness, and the types of services each provides. When accounting for these differences, we urge the Agencies to exclude third-party service providers from the scope of the ANPR.

### 2. Third-Party Service Providers Are Different Than Big Banking Institutions In Many Ways

The covered entities that would satisfy the $50 billion asset threshold are among the largest banking organizations in the world. Indeed, of the 41 U.S. depository institutions that meet the ANPR's size threshold as of September 30, 2016, four have over one trillion dollars in assets and more than half have over $100 billion in assets.[4]

The Agencies, however, do not intend to apply the Standards to all other banking institutions, and it would be unreasonably burdensome for the thousands of banking institutions with less than $50 billion in assets to comply with the Standards. Similarly, it would be unreasonably burdensome to apply the Standards to third-party service providers to the largest banking institutions. Few, if any, such service providers are the size of the covered entities – whether measured by assets, number of employees, resources or any other practical metric. For example, the majority of the covered entities are more than six times larger than Mastercard and some are more than 60 times larger, as measured by assets.

Moreover, few third-party service providers are "interconnected" to the larger financial system in the way that the covered entities are, and the Agencies have not suggested otherwise in the ANPR or elsewhere. "Interconnected" generally implies systemic importance. Indeed, the

---

[2] 81 *Fed. Reg.* at 74,318.

[3] 81 *Fed. Reg.* at 74,316 (emphasis added).

[4] FDIC Institution Directory (January 5, 2017).

Agencies based the ANPR, in part, on guidance intended for systemically important institutions. In preparing the ANPR, the Agencies reviewed and considered the *Guidance on cyber resilience for financial market infrastructures* (the "Guidance").[5] The Guidance is a supplement to the *Principles for Financial Market Infrastructure* ("PFMI").[6] The PFMI are intended to apply to financial market infrastructures that "pose significant risks to the financial system and [can] be a potential source of contagion [if not properly managed], particularly in periods of market stress."[7] In particular, the PFMI are meant to apply to systemically important payment systems.[8] In the U.S., the Financial Stability Oversight Council ("FSOC"), which includes representation from each of the Agencies, is tasked with designating nonbank entities in financial services that are systemically important. With the exception of eight clearinghouses, the FSOC has not determined that any third-party service providers to banking institutions conduct the type of business that would result in being designated as systemically important. Thus, with very limited exception, third-party service providers (including retail payments networks such as Mastercard) do not present a systemic risk to financial markets and should not be subject to requirements that were developed to apply to systemically important institutions.

In addition to size and interconnectedness, third-party service providers are not comparable to covered entities because they generally affect only a small portion of a covered entity's activities. In most cases, a third-party service provider offers a discrete service to each covered entity that affects a narrow portion of the covered entity's business. For example, the retail electronic payments that Mastercard facilitates represent one of many business lines for a covered entity. Covered entities commonly engage in a variety of activities unrelated to retail electronic payments, such as consumer lending, commercial lending, mortgage lending, asset management, derivatives trading, deposit taking, and wholesale payments, plus other types of retail payment business that do not use the services of Mastercard, including checks and, in some cases, private-label credit cards.

By proposing to subject covered entities' third-party service providers to the Standards, the effect of the ANPR is to equate the cybersecurity risks associated with providing a service to a single business line of a covered entity to operating the entire covered entity as a whole. Not to be overlooked, the nature of services across third-party service providers is not uniform. Therefore, the ANPR would impose a regulatory burden on third-party services providers that is vastly disproportionate to the cybersecurity risks that they present to any individual covered entity customer.

### *B. Undue Burden Even If the ANPR Does Not Apply Directly to Third-Party Service Providers*

#### 1. The Challenges of Ongoing Monitoring by Banking Institutions

---

[5] 81 *Fed. Reg.* at 74,317.

[6] CPMI and IOSCO, *Guidance on cyber resilience for financial market infrastructures* 1 (Jun. 2016).

[7] CPMI and IOSCO, *Principles for financial market infrastructures* 5 (Apr. 2012).

[8] *Id.* (emphasis added).

Even if the Agencies determine to exempt third-party service providers from direct application of the Standards, the Standards would still exacerbate the burden on companies that provide services to multiple banks. The External Dependency Management Standard, for example, would obligate banking institutions to perform enhanced ongoing monitoring of their third-party service providers. We are also concerned that banking institutions would attempt to impose other Standards on their third-party service providers, such as the Cyber Risk Management Standard or the Incident Response, Cyber Resilience, and Situational Awareness Standard.

In recent years, the Agencies have substantially increased the supervisory emphasis on banking institutions to manage third-party service providers. An effect of this has been that companies such as Mastercard are subject to contractual audit and reporting requirements from many banking institutions, and those institutions often have varying (and changing) views regarding the nature (scope, depth, *etc.*) of their obligation to conduct audits, require reports and otherwise engage in ongoing monitoring of Mastercard. This translates into a year-round, resource-draining exercise of responding to divergent audit and reporting requests *regarding the same service provided to similarly situated institutions*. We understand that this approach also burdens the banking institutions that must audit each and every one of their third-party service providers. This approach does not benefit banking institutions or the integrity and security of the larger financial system.

### 2. Approach Forward

In lieu of imposing the Standards, we strongly encourage the Agencies to rely on the cyber management standards currently contained in the *FFIEC IT Examination Handbook*. For example, Section II.C.20 of the *Information Security* booklet, entitled "Oversight of Third-Party Service Providers," already sets forth standards for banking institutions to follow in their monitoring of technology service providers. We believe these standards are sufficient to address the cyber risks posed to banks by technology service providers and are more reasonable for companies like ours than the Standards.

If the Agencies do not agree that the standards in the *FFIEC IT Examination Handbook* are sufficient for purposes of enhanced cybersecurity risk management, then we would welcome the opportunity to discuss with the Agencies appropriate cybersecurity measures for technology service providers before the Agencies move forward with the rulemaking. This would give the Agencies an opportunity to receive feedback directly from the industry and afford us the chance to inform the Agencies about the Standards that we believe would be particularly burdensome, including the proposal under the External Dependency Management Standard that would require banking institutions to undertake real-time monitoring of third-party service providers.[9] We would also appreciate the opportunity to discuss with the Agencies the tremendous commitment by our industry to safeguard systems and networks and to implement dynamic, tailored and flexible cyber risk management (and more generally information security) measures that foster the stability of these systems and networks.

---

[9] 81 *Fed. Reg.* at 74,323. Real-time access raises cybersecurity threat issues. For example, if a covered entity is breached, the covered entity could then unwittingly compromise all of the third-party service provider systems to which it is connected for the purpose of real-time monitoring.

Finally, irrespective of the Standards under which the Agencies obligate covered entities to oversee their third-party service providers, we strongly encourage the Agencies to grant covered entities relief from the duty of ongoing monitoring (audits, reports, *etc.*) and testing with respect to the commonly used technology service providers that are examined by the Agencies under the Bank Service Company Act. Review of an examination report from the Federal Financial Institutions Examination Council ("FFIEC") is a practical way for covered entities to understand whether these technology service providers are properly managing cybersecurity, and would also meaningfully reduce the serious burdens discussed above for both banking institutions and those technology service providers examined by the FFIEC.

### *C. Sector-Critical Systems of Covered Entities*

In the ANPR, the Agencies state that they are considering two tiers of Standards, with more stringent standards to apply to systems of covered entities that are critical to the functioning of the financial sector.[10] Among potential "sector-critical" systems, the Agencies are considering whether to classify as "sector-critical" the systems that support the maintenance of a significant share (for example, five percent) of the total U.S. deposits or balances due from other depository institutions in the United States.[11]

To the extent that the Agencies treat as "sector-critical" the deposit systems of banking institutions that have a significant share of U.S. deposits, the Agencies should clarify that debit card networks that facilitate card-based access to those deposits by banking institution customers are not a part of such "sector-critical" systems. Debit card networks such as Mastercard do not accept deposits, do not maintain deposit account records, and do not access deposit accounts. Rather, they process debit card transactions on the basis of a debit card number, which is not the cardholder's deposit account number. In the case of Mastercard, we do so without need of the cardholder's name or other identifying information. Therefore, Mastercard's debit card services are not a part of a bank's deposit operating systems.

Also, the Agencies state that they are considering whether systems that support the clearing or settlement of at least five percent of the value of transactions in certain other markets may be considered sector-critical.[12] The Agencies list the markets for exchange-traded and over-the-counter derivatives as examples. Appropriately, the retail electronic payment market is not listed. As discussed above in the context of systemic importance, retail electronic payments are not a critical financial market and, therefore, should not be considered sector-critical.

Finally, the Agencies propose that any services provided by third parties that support a covered entity's sector-critical systems would be subject to the same sector-critical standards. For the reasons outlined above regarding the issue of application of the Standards to third-party service providers, the Agencies should not apply the heightened sector-critical standards to

---

[10] 81 *Fed. Reg.* at 74,319.

[11] *Id.*

[12] *Id.*

companies that provide services to covered entities with respect to the sector-critical systems of those covered entities.

* * *

Again, Mastercard appreciates the opportunity to provide comments on the ANPR, and we welcome further engagement with the Agencies on this important issue. If there are any questions regarding our comments, please do not hesitate to contact the undersigned at (914) 249-2147 or neil.desai@mastercard.com, or our counsel at Sidley Austin LLP in this matter, Joel D. Feinberg, at (202) 736-8473.

Sincerely,

Neil Desai
Senior Counsel, Regulatory Affairs

cc: Joel D. Feinberg