

MasterCard Worldwide  
Law Department  
2000 Purchase Street  
Purchase, NY 10577-2509  
tel 1-914-249-2000  
www.mastercard.com



December 12, 2007

Ms. Jennifer J. Johnson, Secretary  
Board of Governors of the Federal Reserve System  
20<sup>th</sup> Street and Constitution Avenue, NW  
Washington, DC 20551

Re: Docket Number R-1298

Department of the Treasury  
Office of Critical Infrastructure Protection  
and Compliance Policy  
Room 1327, Main Treasury Building  
1500 Pennsylvania Avenue, NW  
Washington, DC 20220

Re: Docket Number Treas-DO-2007-0015

To Whom It May Concern:

MasterCard Worldwide (“MasterCard”)<sup>1</sup> submits this comment letter in response to the Notice of Joint Proposed Rulemaking (“Proposal”) published by the Board of Governors of the Federal Reserve System and the Department of the Treasury (collectively, the “Agencies”) in the *Federal Register* on October 4, 2007. MasterCard appreciates the opportunity to offer its comments on the Proposal.

### **In General**

MasterCard applauds the Agencies for crafting a Proposal that generally implements the Unlawful Internet Gambling Enforcement Act (“Act”) faithfully and appropriately as it relates to card networks. We believe that, on the whole, the Proposal creates a workable framework for card systems and participants therein to develop reasonable policies and procedures to prevent restricted transactions. We also believe that the Proposal is sufficiently specific to provide card systems and their participants with meaningful compliance objectives without being overly prescriptive.

---

<sup>1</sup> MasterCard Worldwide (NYSE:MA) advances global commerce by providing a critical link among financial institutions and millions of businesses, cardholders and merchants worldwide. Through the company’s roles as a franchisor, processor and advisor, MasterCard develops and markets secure, convenient and rewarding payment solutions, seamlessly processes more than 16 billion payments each year, and provides industry-leading analysis and consulting services that drive business growth for its banking customers and merchants. With more than one billion cards issued through its family of brands, including MasterCard®, Maestro® and Cirrus®, MasterCard serves consumers and businesses in more than 210 countries and territories, and is a partner to 25,000 of the world’s leading financial institutions. With more than 24 million acceptance locations worldwide, no payment card is more widely accepted than MasterCard. For more information go to [www.mastercard.com](http://www.mastercard.com).

As we note in more detail below, however, we believe that some clarifications and slight modifications are appropriate to ensure that we and our customer financial institutions can dedicate our limited resources in the most effective manner to achieve the purposes of the Act and the Proposal. MasterCard also offers comments on specific issues raised by the Agencies in the Proposal. It is important to note that the scope of our comments is limited to issues pertaining to card systems. We offer no comment on other portions of the Proposal, such as those relating to ACH transfers or check collection.

## **§ \_\_.5 Requirement to Have Reasonable Policies and Procedures**

### *General Requirement*

Under the Proposal, all non-exempt participants in a designated payment system (such as a card system) must establish and implement written policies and procedures reasonably designed to identify and block or otherwise prevent or prohibit restricted transactions. MasterCard agrees with this approach in the Proposal. It is important to note that the requirement in the Proposal is to develop and implement certain policies and procedures—it is not a strict prohibition against processing a restricted transaction. A card system would likely not be able to meet such a standard, regardless of its policies and procedures. As the Agencies note in the Supplementary Information, “neither the Act nor the [Proposal] contain specific performance standards but instead require that [a designated payment system’s] policies and procedures be ‘reasonably designed’ to identify and block or otherwise prevent or prohibit unlawful [I]nternet gambling.” We strongly urge the Agencies to retain it in a final rule.

### *Section Heading*

The section heading for § \_\_.5 in the Proposal is “Processing of restricted transactions prohibited.” Assuming the Agencies retain the concept of requiring policies and procedures reasonably designed to prevent restricted transactions—as opposed to an unrealistic prohibition on the processing of such transactions—in a final rule, we believe it would be appropriate to amend this section heading. In fact, and as the Agencies note, neither the Act nor the Proposal would prohibit the processing of restricted transactions. MasterCard suggests the Agencies provide a section heading that is a more accurate descriptor of the section’s requirements, such as “Requirement to Have Policies and Procedures Regarding Restricted Transactions.”

### *Reliance on Payment System Policies*

The Act states that a financial transaction provider is deemed to be in compliance with the final rule if: (i) the provider relies on and complies with the policies and procedures of a designated payment system of which it is a member to identify and block restricted transactions (or otherwise prevent the acceptance of the payment brand in connection with restricted transactions); and (ii) such policies and procedures comply with the final rule. This is an important concept for networks with thousands of participants, such as MasterCard, where such participants all agree to adhere to certain standards as a condition of participating in the network. The Proposal essentially restates this provision almost verbatim. We urge the Agencies to retain this provision in the final rule.

### *Safe Harbor*

The Act provides a safe harbor for any person that blocks or refuses to honor a transaction: (i) that is a restricted transaction; (ii) that such person reasonably believes to be a restricted transaction; or (iii) as a designated payment system, or a member of such system in reliance on the policies and procedures of such system, in an effort to comply with the final rule. This statutory safe harbor ensures that card issuers, merchant acquirers, and the card system itself are not liable in the event that any or all of such parties “overblock” legal transactions in the circumstances described in the Act’s safe harbor (*e.g.*, in an effort to comply with the final rule). This is an important concept because, for a variety of reasons, it may not be clear to a card issuer, card system, or merchant acquirer whether a payment transaction is a restricted transaction or not. For example, none of those parties may know for certain where the cardholder is located at the time of a Internet gambling transaction, and therefore may not know whether the transaction relates to a legal or illegal Internet gambling transaction. As the Agencies have noted in the Supplementary Information, even if jurisdictional questions could possibly be answered, “the Act does not comprehensively or clearly define which activities are lawful and which are unlawful.”

At this time, it may be that an appropriate method to comply with a final rule is to require payment card authorization requests to include transaction codes specifically identifying those requests associated with Internet gambling transactions. Indeed, both the Act and the Proposal contemplate such an approach in complying with the final rule. Although a card system or card issuer may be able to identify an Internet gambling payment transaction through use of such codes, neither party will likely know for certain whether such transaction is actually legal or not. If the transaction involves a U.S.-issued card, it is likely that the card issuer or the card system would simply block or deny authorization for such a transaction, even though there are situations in which such a transaction could—at least in theory—be legal.

If a card issuer or card system blocks a transaction coded as an Internet gambling transaction, and such transaction is not actually a restricted transaction, the statute would shield either party from liability. For example, even if limited amounts of Internet gambling were legal in the U.S. (an assertion the Department of Justice has denied on several occasions, including in congressional hearings), it would not be unreasonable to assume that an attempted Internet gambling transaction on a U.S.-issued card is a restricted transaction. Furthermore, it would seem that the card system’s (or card issuer’s) blocking, based on the coding procedures established by the card system, were done in an effort to comply with the final rule.

We commend the Agencies for intending to “import[] the Act’s liability provisions” into the Proposal. However, the Agencies have redrafted the liability safe harbor such that it differs from the Act, at least in form if not substance. In particular, it is not clear to us whether the third prong of the safe harbor as provided in the Proposal matches the breadth of content of the safe harbor provided in the Act. Although we do not believe the final rule could narrow the statutory safe harbor, we ask the Agencies to restate the safe harbor verbatim from the Act in the final rule for purposes of consistency.

*No Prohibition on Processing Legal Transactions/Mandatory Processing of Gambling Transactions*

The Agencies request specific comment on the Proposal’s approach to ensuring that the Proposal itself does not prevent or prohibit the processing of transactions other than restricted transactions. The Act directs the Agencies to ensure that the final rule does not “prevent[] or prohibit[]” the processing of any transaction in connection with any activity that is not illegal Internet gambling, as defined by the Act. Therefore, according to the Act, the final rule may not prevent or prohibit any transaction other than a restricted transaction. The Agencies could achieve this statutory goal without any explicit reference to it in the Proposal or final rule, and we believe they have done so. However, the Agencies have taken the extra precaution to avoid doubt on this issue by explicitly noting in the text of the Proposal itself that “[n]othing in the [Proposal] requires or is intended to suggest that designated payment systems or participants therein must or should block or otherwise prevent or prohibit any transaction in connection with any activity that is” not a restricted transaction. We believe the Agencies were careful to ensure that the Proposal would not have imposed or suggested such a requirement, but we commend the Agencies for expressly clarifying this matter in the Proposal.

The Act does not require a financial transaction provider to process any otherwise legal transaction. In fact, Congress clearly anticipated that legal transactions would be blocked as a result of the adoption of the final rule, and Congress provided a shield for liability in such circumstances. The plain language of the Act indicates that Congress was concerned only that the scope of the final rule not be broader than requiring policies and procedures pertaining to restricted transactions. Although nothing in the Act requires anyone to process a transaction of any type, we are aware that some may believe that the Agencies should *require* payment systems to process certain types of transactions. As the Agencies correctly state in the Supplementary Information, “the Act does not provide the Agencies with the authority to require designated payment systems or participants in these systems to process any gambling transactions.” Such a requirement would significantly alter the business practices of many financial transaction providers—including the issuers of significant numbers of payment cards who currently routinely decline authorization for *all* transactions on U.S.-issued cards coded as Internet gambling transactions. We believe Congress would have specifically considered and debated the issue and its ramifications had Congress intended to have the Agencies impose such a requirement.

**§ 6. Examples of Policies and Procedures**

*In General*

The Act directs the Agencies to “identify types of policies and procedures, including nonexclusive examples, which would be deemed” to meet the requirements of the final rule. The Proposal includes such examples of policies and procedures that would comply with the final rule. The Proposal also specifically states that the examples are not exclusive, noting that a non-exempt participant in a designated payment system (which includes, by the Proposal’s definition, the designated payment system itself) “may design and use other policies and procedures that are specific to its business and may use different policies and procedures with respect to different types of restricted transactions.” We urge the Agencies to retain the examples in the final rule,

and to continue to state in the final rule that such examples are not exclusive. MasterCard asks the Agencies to clarify, however, that a participant in a designated payment system may design and use other policies and procedures, regardless of whether such policies and procedures are “specific to its business,” as it is not clear what purpose such a limitation serves or how one would determine whether the other policies and procedures were “specific to its business.”

*Card System Examples: Policies and Procedures of Issuers, System, and Acquirers*

The Proposal states that the “policies and procedures of a card system operator, a merchant acquirer, and a card issuer, are deemed to be reasonably designed to prevent or prohibit restricted transactions, if they” meet the standards provided in the card system example. The standards in the example include merchant due diligence, the establishment of transaction codes, denying authorization for restricted transactions, and policing the system. Although we believe these standards are generally reasonable, they are not necessarily the policies and procedures that a merchant acquirer or issuer would implement. For example, a card issuer would not have policies or procedures regarding merchant due diligence. Similarly, a merchant acquirer may not have policies and procedures regarding the denial of authorization of restricted transactions.

The Supplementary Information indicates that the Agencies do not intend to impose obligations on issuers, acquirers, or card systems that are not relevant to the activities of the respective parties. We do not believe the text of the Proposal, however, should suggest that participants in a card system must have policies and procedures that may or may not be applicable to them in order for the overall policies and procedures applicable within a card system to qualify for the safe harbor. Rather, the Agencies should provide an example of policies and procedures that an operator of a card system could implement for purposes of governing its network and allow the network to determine how best to meet those standards. Per the Act and the Proposal, issuers and acquirers would then be able to rely on such policies and procedures for purposes of compliance.

*Card System Examples: Merchant Due Diligence*

As part of the card system example for compliance, the Agencies would require due diligence procedures “designed to ensure that the merchant will not *receive* restricted transactions through the card system.” (Emphasis added.) We applaud the Agencies for noting that the due diligence should be designed to prevent restricted transactions, as opposed to suggesting that the due diligence must ensure that a merchant will not receive restricted transactions.<sup>2</sup> This approach is consistent with the broader requirement to have reasonably designed policies and procedures regarding restricted transactions, as opposed to adopting a strict prohibition with respect to such transactions. We ask the Agencies to clarify, however, that the due diligence process is not intended to prevent the submission of Internet gambling transactions into a card system, but that the process should be designed to ensure that the merchant does not actually receive a payment that is a restricted transaction through the card system.

The Supplementary Information further explains the Agencies’ intentions regarding the due diligence requirements. Specifically, the Agencies state that they “would expect [card

---

<sup>2</sup> We also applaud the Agencies’ expectation, as described in the Supplementary Information, that such due diligence would be performed by the acquirer, not necessarily the operator of a card system.

system] participants' policies and procedures addressing due diligence to be consistent with their regular account-opening practices." Furthermore, the Agencies "anticipate that participants would use a flexible, risk-based approach in their due diligence procedures in that the level of due diligence performed would match the level of risk posed by the customer." MasterCard believes the Agencies have correctly described an appropriate approach to merchant due diligence, and that such expectations should be retained for purposes of the final rule.

With respect to the specific due diligence obligations in the Proposal, MasterCard believes it is appropriate that due diligence be performed on the merchant to ascertain the nature of the merchant's business. We do not believe it is necessary, however, to include "as a term of the merchant customer agreement that the merchant may not receive restricted transactions through the card system." We do not believe such a requirement would add to the effectiveness of the card system example provided by the Agencies. This requirement would also assume that the merchant acquirer is able to determine whether any given transaction is actually a restricted transaction, since the provision would be meaningless if the acquirer were not expected to enforce it. However, an acquiring bank will not know whether a transaction is a restricted transaction since the acquiring bank will not necessarily know the applicable jurisdictions to consider for any given transaction (*e.g.*, such as where the cardholder is located) or the applicable law in such a jurisdiction. On a more practical note, the Proposal would require millions of merchant agreements to be revised. Not only would this create significant compliance burdens—with no improvement in the card system's policies and procedures—but it will also create significant questions between the contracting parties. As the Agencies note, the laws pertaining to the legality of Internet gambling in the United States are not necessarily clear. It would be unreasonable to expect foreign banks and merchants to understand the scope of the proposed contractual term, much less come to a meeting of the minds on it, especially since the requirement would not improve the effectiveness of a card system's policies and procedures.

The Agencies specifically request comment on whether, and to what extent, the examples of due diligence methods should explicitly include periodic confirmation by the participants of the nature of their customers' business. We do not believe the final rule should impose specific recurring timeframes under which a merchant's business must be confirmed. The frequency with which such due diligence may be necessary could vary considerably depending on a variety of factors, and it would be difficult to develop a "one size fits all" approach with respect to ongoing due diligence needs. Consistent with the Agencies' views on due diligence during the account-opening process, any ongoing due diligence procedures must be risk-based and flexible. To the extent the Agencies believe it is necessary to address ongoing due diligence in the final rule, we ask that the final rule simply note that the policies and procedures should address due diligence in establishing and maintaining merchant relationships. The appropriate federal enforcement agencies can then assess the adequacy of such due diligence as part of the overall policies and procedures employed to comply with the final rule.

#### *Card System Examples: Coding and Blocking*

The example for compliance in the Proposal states that the policies and procedures in a card system context should include procedures reasonably designed to identify and block or otherwise prevent or prohibit restricted transactions. Again, MasterCard commends the Agencies for focusing on having reasonable policies and procedures instead of imposing

arbitrary performance standards. We believe this is the appropriate approach, and it should be retained.

As part of such procedures, the Proposal states that the procedures could include establishing transaction codes *and* merchant/business category codes that are required to accompany the authorization request for “a transaction” and creating the operational functionality to enable the card system or card issuer to identify and deny authorization for a restricted transaction. MasterCard agrees with the general concept embodied by this example, but we ask the Agencies to make some minor modifications. First, we do not believe the final rule should specify the type of codes that accompany a transaction (*i.e.*, transaction codes and merchant/business category codes) for purposes of the example so long as the authorization request can be identified as one that may be a restricted transaction. Second, the Proposal should not suggest that specific codes must accompany all transactions, such as those unrelated to Internet gambling, in order to meet the standard provided in the example. Finally, the Proposal suggests that the coding system should “enable the card system or the card issuer to identify... a restricted transaction.” For the reasons described above, neither the acquirer, card system, nor the issuer will necessarily be in a position to determine whether a transaction is actually a “restricted transaction” regardless of the codes used. We believe the final rule should clarify that the codes enable the card system or the card issuer to identify a transaction “that may be a restricted transaction.”

#### *Card System Examples: Ongoing Monitoring or Testing*

As part of the Proposal’s treatment of identifying and blocking (or otherwise preventing) restricted transactions, the card system example includes “[o]ngoing monitoring or testing to detect potential restricted transactions.” The Proposal then suggests that such monitoring or testing could include any one of three options: (i) transaction testing to evaluate the proper coding of transactions; (ii) monitoring web sites to detect unauthorized use of the card system, including its trademark; or (iii) monitoring and analyzing payment patterns to detect suspicious payment volumes from a merchant.

MasterCard concurs with the Agencies that policies and procedures reasonably designed to prevent restricted transactions should include a mechanism to ensure that a card system’s network rules relating to restricted transactions are applied appropriately. We also believe that options such as transaction testing or merchant monitoring may be reasonable methods for a network and/or its participants to use for those purposes. It may also be appropriate to determine whether rogue merchants have gained unauthorized access to the card system. If the merchant uses a card system’s trademark on its web site, but is not accepting the card system’s payment cards, we question whether the monitoring of such site’s trademark violations would serve as an effective means of “monitoring or testing to detect potential restricted transactions” through the card network. Although we discuss issues relating to trademark violations and similar issues in more detail below, we do not believe the Agencies should suggest that monitoring such violations is necessary for purposes of transaction monitoring or testing.<sup>3</sup>

---

<sup>3</sup> The Agencies provide an example in the Supplementary Information of how such monitoring of trademark violations could serve as a transaction monitoring tool in the context of money transmitters. The example appears to

### *Card System Examples: Enforcement*

The card system example of policies and procedures reasonably designed to prevent restricted transactions in the Proposal includes enforcement mechanisms for those policies and procedures. Specifically, the safe harbor in the Proposal states that there should be procedures with respect to a merchant if the card system, card issuer, or merchant acquirer becomes aware that a merchant has received a restricted transaction. These procedures could include fines or denial of access to the network.

MasterCard agrees with the Agencies that policies and procedures reasonably designed to prevent restricted transactions should include provisions to enforce those policies and procedures. However, it appears that the Agencies envision a situation in which the merchant is to be penalized for receiving a restricted transaction, regardless of whether the merchant's transaction is properly coded. In this regard, the Proposal's examples of fines and expulsion appear to relate to "procedures to be followed with respect to a merchant customer." We agree that the operator of a card system should have an enforcement scheme for its policies and procedures to prevent restricted transactions, and that such enforcement scheme could allow for fines and/or expulsion as appropriate. MasterCard is concerned, however, that the Agencies expect MasterCard to hold a merchant liable if the merchant receives a restricted transaction, even if the transaction were properly coded. We believe the example of enforcement mechanisms should recognize that a card system's rules may impose appropriate penalties against a variety of parties depending on which party did not comply with the network's rules to prevent restricted transactions.

Although the Agencies do not appear to include such a requirement in the Proposal's card system compliance example, the Supplementary Information states that the Agencies also expect a card system "to take appropriate remedial action" with respect to an Internet casino that is using the card system's trademark to "promote" restricted transactions. The Supplementary Information also states that the card system could, for example, take legal action to prevent unauthorized use of its trademark by such Internet casino. We caution the Agencies against any suggested or actual requirement that a card system (or any financial transaction provider) expend scarce resources to take "remedial action" against any Internet casino web site that makes unauthorized use of the system's trademarks. MasterCard deplors the unauthorized use of its trademark and takes appropriate steps to prevent and remediate trademark and similar violations. Given the nature of the Internet, however, it can be extremely difficult to determine who is operating an offending web site if the operator is not a merchant within our system. Even if it were possible to locate a party to hold accountable for a trademark violation, it can be extremely costly to attempt to litigate or take other remedial action against such a party, assuming we have any meaningful recourse at all against the offender. Any suggestion that MasterCard is expected to investigate and prosecute all Internet casinos' unauthorized use of its marks could divert enforcement resources from more pressing and fruitful enforcement strategies.

### **Creating "Legal" and "Illegal" Gambling Codes**

---

relate, however, primarily to unauthorized access to the payment system as opposed to whether or not a web site is simply making unauthorized use of a trademark.

In the Supplementary Information, the Agencies state:

Card systems may be able to develop one or more merchant category codes for gambling transactions that are not restricted transactions under the Act. For example, in certain cases it may be reasonably practical for card systems to develop merchant category codes for particular types of lawful Internet gambling transactions. The Agencies specifically seek comment on the practicality, effectiveness, and cost of developing such additional merchant codes.

Although this topic will likely garner discussion among financial transaction providers once a final rule is issued, it is not clear to us that this is a matter that should affect the Agencies' development of a final rule. As we discuss above, the Agencies' task under the Act is limited to ensuring that designated payment systems and their participants have policies and procedures reasonably designed to prevent restricted transactions. Whether or not such policies and procedures may result in additional legal transactions being blocked does not appear to have any bearing on the congressional directive to the Agencies, other than to ensure that the final rule itself does not require the blocking of legal transactions. Therefore, we assume the Agencies' request for comment on this topic is more of an academic exercise than one that would have an impact on the final rule.

At this time, it is not clear to MasterCard whether appropriate codes—or other mechanisms—could be developed to block (or allow issuers to block) only those transactions that are actually restricted transactions. Among the difficulties with developing such an approach is evaluating and understanding the legality of any given Internet gambling transaction.<sup>4</sup> At the very least, the legality of some Internet gambling transactions in the U.S. appears to be a topic of intense debate and one upon which even the Agencies have expressly declined to opine. Even if MasterCard were certain of the Internet gambling laws in each U.S. jurisdiction, there is currently no capability for a card system (or its participants) to determine with certainty where a cardholder is located at the time he or she engages in an Internet gambling transaction. Such a determination would be critical in at least some transactions for purposes of determining whether the Internet gambling transaction is a restricted transaction or not.

Having said this, MasterCard intends to review its compliance with any final rule on an ongoing basis to ensure not only our compliance with the law, but also to evaluate how we may serve the legitimate needs of our financial institution customers and our cardholders. We may determine that there are mechanisms that allow us to refine the scope of a coding and blocking scheme, or any other method used to comply with a final rule. For example, if it were clear from the Department of Justice and other relevant agencies that certain types of Internet gambling were legal, we would explore the feasibility (practical, commercial, and otherwise) of developing a mechanism that allowed issuers to distinguish authorization requests relating to such transactions from those relating to Internet gambling transactions that are more likely to be restricted transactions. MasterCard respectfully suggests, however, that this should not be an issue subject to rulemaking or affecting the outcome of the final rule.

---

<sup>4</sup> We note that the difficulties mentioned by the Agencies in developing a “black list” of unlawful Internet gambling sites are equally applicable if MasterCard were expected to determine the legality of a merchant's gambling operations, *i.e.*, it would require significant investigation and legal analysis for each merchant.

## **Creation of a “Black List”**

The Agencies request comment on whether the creation of a “black list” of “unlawful Internet gambling businesses” would be appropriate. The Supplementary Information describes the many obstacles the Agencies would face in trying to create such a list. Aside from those obvious difficulties, we believe other issues also make such a list unappealing. It is not clear, for example, how an Internet casino would qualify for such a list. There are Internet casinos that operate legally in their home jurisdiction, such as the United Kingdom. We doubt that the Agencies would attempt to place all such Internet casinos on a black list, as such a list would eliminate the ability of U.S. financial transaction providers to serve such legal entities in connection with their legally permissible activities. Such a result would represent a drastic leap from the mandate in the Act. Therefore, the Agencies would likely need to develop a list based on additional, subjective factors.<sup>5</sup> Would the list be comprised of web sites that have ever accepted a single restricted transaction, or would there be a more detailed evaluation of a web site’s activities? How would a black-listed web site have itself removed from the list if it were willing to abide by a designated payment system’s policies and procedures to prevent restricted transactions?

Assuming the Agencies could resolve the issues surrounding the creation and maintenance of a black list, it is not clear what benefit the list would provide. We believe the most appropriate means to achieve the goals in the Act relating to card systems are generally those the Agencies have proposed. If, despite the reasonable efforts of a card network and its participants, an Internet casino is still able to receive significant numbers of restricted transactions, certainly such casino would also know how to use multiple names so as to avoid appearing on a cumbersome list that is obsolete the day it is published. In this regard, a black list adds little value but significant compliance obligations for thousands of merchant acquirers.

## **Effective Date**

The Agencies propose to make the final rule effective six months after it is published. If the Agencies were to incorporate our comments into the final rule, we believe a compliance timeframe of nine months would be reasonable for purposes of card systems.<sup>6</sup> In this regard, MasterCard has developed the infrastructure to implement written policies and procedures reasonably designed to prevent restricted transactions as exemplified in the Proposal. Our customer financial institutions would likely be able to rely on and implement such policies and procedures relatively expeditiously. However, if the Agencies do not adopt our relatively minor suggestions, we and our financial institution customers could need up to 18 months to comply with a final rule. For example, if the text of the final rule continues to suggest that each issuer and acquirer must have its own policies and procedures addressing all issues relating to a card system, as opposed to allowing issuers and acquirers to limit the scope of their programs or to rely on the network’s program, developing a strategy to comply with the final rule could be a cumbersome and difficult process for card networks, issuers, and acquirers. Furthermore, if the Agencies implicitly require acquirers to revise contracts with merchants for purposes of the safe

---

<sup>5</sup> It is important to emphasize that, should a list be part of any final rule, the list must be developed by the federal government and not the private sector.

<sup>6</sup> This may or may not be a reasonable timeframe for other designated payment systems.

harbor, it is unlikely that millions of contracts could be revised within six months (if such a goal could be achieved at all). The development of a comprehensive program to identify trademark violators around the world, and to prosecute such violators in dozens of jurisdictions, would also take significant time and effort.

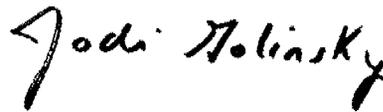
**Conclusion**

We commend the Agencies for developing a sound, workable Proposal for card systems to develop policies and procedures reasonably designed to prevent restricted transactions. Although we offer several comments above, we do not believe the Proposal requires significant substantive revision or modification with respect to card systems to achieve the goals prescribed in the Act. MasterCard respectfully urges the Agencies to make the relatively minor clarifications and modifications described above so that MasterCard and our customer financial institutions can comply with the final rule efficiently and effectively.

\* \* \* \* \*

Once again, we appreciate the opportunity to comment on the Proposal. If you have any questions concerning our comments, or if we may otherwise be of assistance in connection with this issue, please do not hesitate to call me at (914) 249-5978 or our counsel at Sidley Austin LLP in connection with this matter, Michael F. McEneney at (202) 736-8368 or Karl F. Kaufmann at (202) 736-8133.

Sincerely,



Jodi Golinsky  
Vice President &  
Regulatory and Public Policy Counsel

cc: Michael F McEneney, Esq  
Karl F. Kaufmann, Esq.