Joshua L. Peirez
Vice President &
Senior Legislative/Regulatory Counsel

MasterCard International
Law Department
2000 Purchase Street
Purchase, NY 10577-2509
914 249-5903
Fax 914 249-4261
E-mail joshua_peirez@mastercard.com
Internet Home Page:
http://www.mastercard.com

10

MasterCard International

Via Electronic Mail

May 29, 2002

FinCEN
Post Office Box 39
Vienna, VA 22183

Attention: Section 352 CC Regulations

Dear Sir:

This comment letter is submitted on behalf of MasterCard International Incorporated ("MasterCard") in response to the Interim Final Rule ("Rule") published by the Financial Crimes Enforcement Network ("FinCEN") of the U.S. Treasury Department to provide guidance to operators of credit card systems ("operators") regarding their anti-money laundering obligations under the Bank Secrecy Act ("BSA"). MasterCard commends FinCEN for its efforts in developing the Rule and appreciates the opportunity to submit these comments.

BACKGROUND

The MasterCard System

MasterCard is a global membership organization comprised of financial institutions that are licensed to use the MasterCard service marks in connection with a variety of payments systems. These member financial institutions issue payment cards to consumers and contract with merchants to accept such cards. MasterCard provides the networks through which the member financial institutions interact to complete payment transactions—MasterCard itself does not issue payment cards, nor does it contract with merchants to accept those cards.

Recent Anti-Money Laundering Efforts

Shortly after the events of September 2001, MasterCard began to examine ways that it could play a role in fighting terrorism. Initially, these efforts focused on issues specifically related to September 11, such as assisting in the many ongoing investigations by federal law enforcement agencies, waving transaction fees associated with charitable contributions to September 11 charities paid by

MasterCard cards, and working on issues related to postal disruption resulting from the anthrax mailings last fall. The focus soon expanded to examining ways in which MasterCard could strengthen its own procedures to protect against terrorists and money launderers gaining access to the MasterCard systems. These efforts further crystallized with the enactment of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act").

MasterCard quickly recognized that any useful effort would involve many parts of the MasterCard organization and would require substantial cross-functional cooperation. As a result, in January, MasterCard formed a multi-disciplinary task force ("Task Force") to address efforts to prevent money laundering and the financing of terrorism through misuse of the MasterCard system. The Task Force, which reports directly to senior management, is comprised of representatives of the Law Department, Security and Risk Department, Licensing, Risk Management, Global Technology and Operations, our Regional offices, and our Member account management. The primary efforts of the Task Force have been focused on developing and refining MasterCard's anti-money laundering program. In addition, the Task Force began the process of informing the employees of MasterCard regarding the importance of MasterCard's role in fighting money laundering and terrorism. For example, in February 2002, the co-chairs of the Task Force and the general counsel of MasterCard gave a presentation to more than 700 MasterCard employees highlighting MasterCard's efforts to address terrorism and money laundering and alerting employees to their responsibility to assist in these efforts. Other presentations and employee communications continue and will be increasingly formalized over time.

In short, MasterCard is committed and well prepared to do its part in fighting money laundering and terrorism. We believe that the Rule provides important guidance regarding how MasterCard can fulfill that role and we commend FinCEN for its efforts in developing the Rule. As discussed below, the Rule sets forth an efficient, sensible approach for an operator to use in developing and maintaining an anti-money laundering program, and provides the essential flexibility that is needed to combat money launderers efficiently as they evolve their efforts to gain access to payments systems. The following discusses our more specific comments regarding the Rule.

SPECIFIC COMMENTS

Supplementary Information

Section I.A. Credit Card Systems

This subsection provides a good overview of the separate roles of issuing and acquiring members in a payment system such as MasterCard. As a general

matter, it also provides an accurate description of the functions performed by an operator. One clarification we would suggest, however, involves the discussion of the "settlement process." Specifically, FinCEN states that as part of the settlement process in a credit card system, "[t]he operator [of the system]...transmits the funds to the merchant bank in settlement of the debt." In practice, the funds are actually transmitted by depository institutions based on instructions from the operator. The operator's instructions only relate to transfers from the issuer. We urge FinCEN to revise this portion of the discussion accordingly in the next iteration of the Rule ("Amended Rule").

Section I.B. The Authorization of Acquiring and Issuing Banks

This section describes the role that an operator plays in authorizing issuing and acquiring institutions to participate in the system. It states, for example, that while issuing institutions are responsible for their relationships with cardholders and acquirers for theirs with merchants, "[t]he operator of the system is directly responsible for selecting and approving issuing and acquiring institutions to become part of the system, and setting the rules by which they must abide." This distinction is an important one and provides the foundation for the thrust of the Rule. We believe, however, that one clarification to this subsection would be necessary to avoid confusion regarding an operator's relationship with cardholders and merchants. Specifically, the subsection states that "in its role of ensuring that the member institutions continue to abide by the membership rules, the operator...indirectly plays a role in selecting and approving other users in the system, including cardholders and merchants." MasterCard is concerned that this sentence overstates the role of an operator with respect to cardholders and merchants. In particular, although MasterCard has established standards that acquirers should use in establishing their relationships with merchants, MasterCard does not play a role in "selecting" or "approving" either merchants or cardholders. We believe that other sections of the Rule and Supplementary Information recognize this distinction and that confusion on this point could lead to an operator such as MasterCard having to "regulate" the member financial institutions in contradiction to FinCEN's stated objective of avoiding that outcome.

Section I.C. Existing Anti-Fraud Functions Performed by the Operator of a Credit Card System

In this subsection, FinCEN correctly observes that "[i]ncentives exist for the operator of a credit card system to minimize financial losses caused by fraud in connection with use of its credit card" and that "these incentives encourage operators to scrutinize institutions" for potential fraud and economic risks before admitting them into the system. The Rule "seeks to take advantage of those existing practices by increasing the scope of the due diligence conducted by the operator to include the potential for money laundering or terrorist financing." This approach is critically important and should be retained in any Amended Rule. In

this regard, it is essential that operators are able to implement their anti-money laundering programs as efficiently as possible so that internal resources can be devoted to those activities likely to produce the best results. The Rule greatly facilitates this objective by allowing operators to build on their existing due diligence functions to address money laundering issues rather than requiring them to develop entirely new processes or departments.

MasterCard believes that this due diligence approach is, and will be, the cornerstone for successful anti-money laundering programs for MasterCard and other operators. At the same time, MasterCard recognizes that money launderers, like the many other types of criminals we have battled over the years, are likely to evolve and become more sophisticated in their efforts to avoid detection. As a result, MasterCard will continue to analyze new ways to combat the problem. However, as noted in the Rule, we do not presently believe that any transaction monitoring systems exist that would be effective enough with respect to terrorist financing and money laundering to warrant the dedication of resources to them. Accordingly, we concur with FinCEN's decision to not require operators to monitor individual transactions to detect potential money laundering or terrorist financing at the present time.

Section I.D. Money Laundering and Terrorist Financing Risks Associated with Credit Cards from the Perspective of the Operator of a Credit Card System and Section I.E. The Anti-Money Laundering Program

Section I.D. states that the primary focus of the Rule "is on the risks—and the need to minimize them—associated with the authorizing, and maintaining authorization for, issuing and acquiring institutions." Section I.E. then clarifies the basic elements of an operator's anti-money laundering program. It states that "the anti-money laundering program required by this [Rule] is designed primarily to ensure that operators of credit card systems conduct sufficient due diligence on those banks or other entities that they authorize to be issuing or acquiring institutions." It also clarifies that "[s]uch due diligence should be performed prior to accepting the institution into the system, and on an on-going basis with a frequency that is commensurate with the risk posed by the particular institution." An operator's program also must have "procedures to minimize the opportunity for money laundering or terrorist financing when identified high-risk institutions" participate in the system. In addition, "it is expected that operators will tailor existing rules and guidelines governing member institutions to minimize the risk of money laundering or terrorist financing." MasterCard believes that these elements form the basis for an effective anti-money laundering program and has developed its own program with similar elements in mind. Perhaps most important is FinCEN's clarification that "the program should be risk-based, meaning that resources should be devoted to those areas that pose the greatest risk of money laundering or terrorist financing." This clarification is especially important in connection with an operator's phased review of its currently existing member base

(which in the case of MasterCard exceeds 15,000 institutions worldwide) in the first instance. Given the enormity of this task, we strongly urge FinCEN to maintain this approach in order to ensure that operators can target high risk areas first and foremost and are not forced to devote unwarranted resources to efforts which may produce relatively negligible results.

Section I.E. also provides helpful clarification regarding the contours of the Rule. Specifically, Section I.E. states:

> The focus of the [Rule] is on what operators can and do control....The [Rule] is not intended to place the operator of a credit card system in the role of guaranteeing that no issuing or acquiring institutions permit money laundering or terrorist financing through the use of the operator's credit card. To the contrary, while the operator of the credit card system will play an important role in minimizing the risk of abuse by controlling access to the system, perhaps even denying access to institutions posing an unreasonable risk of money laundering or terrorist financing, the operator should not be placed in the role of regulating issuing or acquiring institutions.

Additionally, section I.E. encourages operators to have procedures in place for voluntarily reporting suspected terrorist activity to FinCEN through its Financial Institutions Hotline. MasterCard supports efforts to encourage voluntary reporting of suspected terrorist activities and intends to continue its own efforts to do so. We believe, however, that more must be done to eliminate potential legal obstacles to such voluntary reporting and we urge Treasury to take additional steps in this area. In particular, as we indicated in our comment letter to FinCEN regarding its proposed regulations implementing Section 314 of the USA PATRIOT Act, we urge FinCEN to adopt a comprehensive safe harbor for any financial institution that voluntarily provides information to FinCEN or other financial institutions regarding suspected terrorist or related activity. Such a safe harbor is critically important to ensure that those who undertake to assist in the war on terrorism are not subject to liability for doing so. Indeed, MasterCard urges FinCEN to also adopt a safe harbor for operators that reject, refuse, or terminate financial institutions based on money laundering concerns. Such a safe harbor should also recognize that various local laws around the world may provide penalties for terminating or denying relationships on such a basis and should deny the enforceability of any judgments in the United States on such basis.

The Rule

Adopting a Program

Under the Rule, each operator must develop a written anti-money laundering program reasonably designed to prevent its system from being used to

facilitate money laundering and the financing of terrorist activities. The Rule states that the program must be in writing and approved by "senior management." Given the significance of the issues addressed by an operator's program, MasterCard believes it is appropriate that the program be approved by senior management. However, we urge FinCEN to refrain from adopting more prescriptive guidance with respect to the involvement of senior management to ensure that operators have the flexibility to adapt quickly to changing money laundering schemes. For example, it may become necessary for an operator to amend its program on short notice to address a newly discovered money laundering approach and operators should be free to designate the members of senior management who will be available to review and approve such changes.

Again, MasterCard commends FinCEN for its recognition in the Supplementary Information to Section 103.135(b) that the Rule is designed to allow operators the flexibility to design their programs to meet the specific risks presented. We believe this is a most effective approach, avoiding a "one size fits all" remedy to a problem that is best addressed based on the unique circumstances surrounding each operator. For example, the contents of a program could depend on an operator's membership process, member activities, or scope of operations. By allowing operators the ability to tailor their programs to the specific risks presented, the Rule will allow each operator to design a program that most effectively and efficiently addresses its identified risks, as opposed to imposing a more rigid approach that may require dedicating resources to efforts that are unlikely to produce appreciable benefits, thereby taking away resources from more fruitful efforts.

We also concur with FinCEN's observation that the risks posed by a member institution may be minimal if the institution does not fall within a high risk category. This undoubtedly would be true, for example, with respect to the large majority of member institutions located in the U.S., each of which must comply with its own anti-money laundering requirements and is subject to regulation, examination, and supervision by federal regulatory agencies. It also would be true with respect to many of the foreign members of MasterCard, particularly those that are subject to the strict anti-money laundering requirements of their own countries, such as those that are members of the Financial Action Task Force on Money Laundering. In this regard, we agree with FinCEN's acknowledgement that "[t]he fact that a member institution is a foreign bank or entity is not itself determinative of the risk posed." Indeed, a proper risk assessment will evaluate the circumstances involving each institution. Such assessment will undoubtedly involve an evaluation of the jurisdiction in which the institution is chartered or regulated, but the fact that it may be outside the United States is not a *per se* indication of increased risk.

Effective Date

The minimum standards for the program in the Rule become effective July 24, 2002. Although MasterCard has been working aggressively on this issue for eight months and developed its initial program to meet the deadline imposed by Section 352 of the USA PATRIOT Act, we urge FinCEN to delay the effective date of the Rule for an additional 5 months until December 24, 2002. This would allow sufficient time to enable each operator to implement and test its program and to work with the Treasury Department to address any questions or issues that have arisen. In this regard, operators may need additional time to review the Rule and adjust their programs in a thoughtful manner in light of some of the detail provided in the Rule that was not present in the USA PATRIOT Act, itself. As FinCEN notes in the Rule, the BSA requirement for an anti-money laundering program has not applied to operators until now. As such, operators have an enormous task to undertake in a variety of areas including, policy development, employee education materials development, staffing decisions, and implementation. Operators should have more than only three months[1] to digest the contents of the Rule, evaluate their current programs, and implement any necessary changes. Therefore, we believe the Amended Rule should be effective no earlier than December 24, 2002.

Policies, Procedures, and Internal Controls

The Rule requires an operator's program to include policies, procedures, and internal controls focused on the process of reviewing the risks of participation by issuing and acquiring institutions. The Supplementary Information indicates that FinCEN expects this to "involve the operator adapting existing licensing or membership agreements to ensure that member banks and entities fulfill their obligations to assist the operator in guarding against money laundering and terrorist financing." This requirement is a distinct departure from FinCEN's general belief that each operator should have the flexibility to design a program based on its unique circumstances. We respectfully suggest that FinCEN modify this statement to suggest that operators consider rule changes and/or contractual agreements with their members to mitigate the potential for money laundering or terrorist financing. Whether rules and/or agreements are necessary would depend on the operator's overall risk assessment with respect to the existing or potential member.

The Supplementary Information also notes that the frequency with which members are to be reviewed to ensure compliance with the operator's program will depend on the operator's risk assessment with respect to the particular member. This is an important clarification and we urge that it be retained in any Amended Rule. For example, an operator may not need to review the status of a small

---

[1] The Rule was published in the *Federal Register* on April 29, 2002 and compliance is required by July 24, 2002.

federally insured depository institution with no international operations as often, or to the same extent, as a newly chartered foreign institution with operations in a jurisdiction that does not have as robust a set of anti-money laundering regulations as the United States.

Risk Assessment

FinCEN anticipates that an operator's risk assessment with respect to money laundering and terrorist financing posed by an existing or potential member would include many of the same factors that bear on whether the institution represents a risk of fraud or insolvency. MasterCard agrees. Many of the factors used to evaluate risk of fraud or insolvency (*e.g.* quality of management, financial condition of the institution, the regulatory regime in the chartering jurisdiction) will undoubtedly prove useful in evaluating the institution's risk with respect to money laundering or terrorist financing.

It is also true that operators will need to consider information provided by Treasury, FinCEN, and other U.S. government sources. In fact, the federal government and international organizations will most likely be a key source of information with respect to an operator's risk assessment. The U.S. government and international organizations (*e.g.* the Financial Action Task Force on Money Laundering and OECD more generally) are in a better position to evaluate certain critical risk factors that an operator will likely consider in its risk assessment, such as whether government investigations suggest the institution is participating in terrorist financing and whether the institution's home jurisdiction cooperates with international money laundering initiatives. We also concur with FinCEN's observation that publicly available information, such as public regulatory information or press coverage involving the institution, should be considered.

Presumed Heightened Risks

The Rule states that certain institutions, such as certain foreign shell banks or banks operating under an offshore banking license, are presumed to pose a heightened risk of money laundering or terrorist financing. However, FinCEN specifically states that "even though there is a presumption of a heightened risk, operators still retain the flexibility to assess the risk posed in each case." It is critically important that FinCEN maintain this position with respect to any Amended Rule. Although the heightened risk will require operators to evaluate the institution's risk to the system more extensively, further examination may indicate that the institution does not pose a significant risk to the operator. For example, although a financial institution may be located in a *jurisdiction* that has been designated as noncooperative with international anti-money laundering principles, the *institution* itself may have gone to lengths to take the proper measures to mitigate the risk of money laundering or terrorist financing, or may be willing to undertake such efforts in order to gain or retain access to the operator's systems.

Compliance with the Bank Secrecy Act

The Rule states that operators must comply with any applicable provisions of the BSA or the implementing regulations. We urge FinCEN to delete this provision. We are concerned that the provision could create the false implication that operators may have obligations under current law that they do not have. We note that the Supplementary Information states that "this provision is inserted in the [Rule] in the event future BSA requirements are imposed on operators of credit card systems." We believe it would be more appropriate to address the applicability of future requirements to operators at the time any such requirements are imposed.

Compliance Officer

Under the Rule, operators must designate a compliance officer who is responsible for implementing the program effectively, updating the program as necessary, and providing training to appropriate personnel. We believe these responsibilities are appropriate for the compliance officer. MasterCard is concerned, however, that language in the Supplementary Information may unnecessarily limit the pool of candidates eligible for the job. Specifically, the Supplementary Information states that the compliance officer must be "knowledgeable regarding BSA requirements and money laundering issues and risks" without recognizing that other factors may be just as important, if not more so. For example, knowledge of the operator's business and the business of its members, or previous experience with regulatory compliance matters would be important characteristics of a strong candidate for the compliance officer position. A candidate possessing these characteristics would be well prepared to assess how the operator's system may be at risk for use by money launderers, even if the candidate did not have prior experience with the BSA. In order to ensure that the pool of qualified candidates is not artificially restricted, we urge FinCEN to clarify that an individual could be eligible to serve as the compliance officer if the individual has the appropriate qualifications *to become* knowledgeable regarding BSA requirements and money laundering issues. Indeed, it may be easier to become knowledgeable regarding BSA requirements and money laundering issues than it is to acquire the necessary understanding of the operator's system and its component parts.

Audits

An operator's program must provide for an independent audit to monitor and maintain an adequate program. The Supplementary Information clarifies that although the Rule refers to an "audit," the term does not mean a financial audit and need not be performed by an outside consultant or accountant. This clarification indicates that the intent of the Rule is for operators to perform, or have performed, a *compliance* audit with respect to the program. The Rule also states that the

scope and frequency of the audit shall be commensurate with the risks posed by the operator's members. These clarifications are extremely important and should be retained.

* * * * *

Once again, MasterCard appreciates the opportunity to comment on this important matter and takes its obligations in this ongoing issue very seriously. We also reassert our support for the overall approach taken in the Rule and offer our assistance to FinCEN in further developing the Rule. 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 the number indicated above, or Michael F. McEneney, our counsel in connection with this matter, of Sidley Austin Brown & Wood LLP at (202) 736-8368.

Sincerely,

Joshua L. Peirez
Vice President &
Senior Legislative/Regulatory Counsel

cc: Michael F. McEneney, Esq.