BILLING CODE 4810-02

DEPARTMENT OF THE TREASURY

31 CFR Part 103

RIN 1506-AA28

Financial Crimes Enforcement Network; Anti-Money Laundering Programs for Operators of a Credit Card System.

AGENCY: Financial Crimes Enforcement Network (FinCEN), Treasury.

ACTION: Interim final rule.

SUMMARY: FinCEN is issuing this interim final rule to define and provide guidance to operators of credit card systems concerning the revised provision in the Bank Secrecy Act that requires them to establish anti-money laundering programs.

DATES: This interim final rule is effective April 24, 2002. Written comments may be submitted to FinCEN on or before [INSERT DATE THAT IS 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: Submit comments (preferably an original and four copies) to FinCEN, P.O. Box 39, Vienna, VA 22183, Attn: Section 352 CC Regulations. Comments may also be submitted by electronic mail to regcomments@fincen.treas.gov with the caption in the body of the text, "Attention: Section 352 CC Regulations." Comments may be inspected at FinCEN between 10 a.m. and 4 p.m. in the FinCEN Reading Room in Washington, D.C. Persons wishing to inspect the comments submitted must request an appointment by telephoning (202) 354-6400 (not a toll-free number).

FOR FURTHER INFORMATION CONTACT: Office of the Chief Counsel (FinCEN),

(703) 905-3590; Office of the Assistant General Counsel for Enforcement (Treasury), (202) 622-1927; or the Office of the Assistant General Counsel for Banking & Finance (Treasury), (202) 622-0480 (not toll-free numbers).

SUPPLEMENTARY INFORMATION:

I. Background

On October 26, 2001, the President signed into law the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 (Public Law 107-56) (the Act). Title III of the Act makes a number of amendments to the anti-money laundering provisions of the Bank Secrecy Act (BSA), which are codified in subchapter II of chapter 53 of title 31, United States Code. These amendments are intended to make it easier to prevent, detect, and prosecute international money laundering and the financing of terrorism. Section 352(a) of the Act, which becomes effective on April 24, 2002, amended section 5318(h) of the BSA. As amended, section 5318(h)(1) requires every financial institution to establish an anti-money laundering program that includes, at a minimum, (i) the development of internal policies, procedures, and controls; (ii) the designation of a compliance officer; (iii) an ongoing employee training program; and (iv) an independent audit function to test programs. As operators of credit card systems are identified as financial institutions under the BSA, 31 U.S.C. 5312(a)(2)(L), they are subject to the anti-money laundering program requirement. This rule is intended to define an "operator of a credit card system," and to provide guidance to them in complying with the law, tailored to the industry.

A. Credit Card Systems

Credit cards represent the right to purchase goods and services, or in some cases the right to obtain a cash advance, against a line of credit offered by the issuer of the credit card. The

Truth in Lending Act defines a credit card as a "card, plate, coupon book or other credit device existing for the purpose of obtaining money, property, labor, or services on credit."[1] 15 U.S.C. 1602(k). This interim final rule adopts this definition. Also included within this definition is a charge card, that is, a credit card for which the cardholder must pay the monthly balance in full.[2]

The use to which a credit card may be put depends upon the entity issuing or accepting the card.[3] In the case of general purpose credit cards, such those issued by members of the VISA or MasterCard system, the cards are accepted by a variety of merchants worldwide. In the United States, most such cards are issued by banks[4] authorized by the operator of the credit card system to use the particular name and access the associated clearance and settlement system. Such entities are called "issuing institutions." On the other side of the transaction, in order for a particular merchant to accept the credit card, it must have a relationship with a bank or entity that is itself authorized to sign up merchants to accept the credit card for purchases and process such credit card transactions. Entities authorized to accept credit card purchases from merchants are called "acquiring institutions" or "merchant institutions." In all cases, the operator of the credit card system determines which entities may serve as issuing and acquiring institutions (member institutions) and prescribes rules that member institutions must follow.

Other credit cards used in the United States are issued by a particular merchant or vendor and may only be used in connection with purchases made from that merchant or vendor.

---

[1] "Credit" is defined as "the right granted by a creditor to a debtor to defer payment of a debt or to incur debt and defer its payment." 15 U.S.C. 1602(e).

[2] Regulations implementing the Truth in Lending Act define a charge card as "a credit card on an account for which no periodic rate is used to compute a finance charge." 12 CFR 226.2(15). This interim final rule likewise adopts this definition.

[3] In its 1997 report entitled, "Payments, Clearance, and Settlement: A Guide to the Systems, Risks and Issues," the General Accounting Office described the use of credit cards generally, as well as the role of operators of a credit card system in the clearance and settlement of transactions. *See* GAO/GGD-97-73 at 108-15 (June 1997) ("the 1997 GAO Report").

[4] For purposes of this preamble, the term "bank" refers to insured depository institutions, including federally and state chartered banks, thrifts, and credit unions.

Examples include department store and oil company credit cards, as well as charge cards issued by individual merchants. Often such cards are issued by a bank on behalf of a particular merchant, but in some cases the merchant itself may issue the card. Merchants, vendors, or banks whose issuance of credit cards is restricted to such circumstances do not fall within the definition of an operator of a credit card system as set forth in this interim final rule.[5] However, if an entity otherwise falls within the definition of an operator of a credit card system under this interim final rule, the fact that the operator may also issue credit cards with particular merchants, or may itself serve as the issuing or acquiring institution, does not remove it from the scope of this interim final rule.

The purpose for distinguishing between general purpose credit cards and merchant cards lies first in the fact that the definition in the BSA refers to "an operator of a ***credit card system"*** as a financial institution. We do not view the issuance of a merchant or vendor card as the operation of a credit card system, which is more naturally interpreted to refer to the organizer of a membership or other interrelated group. Second, as discussed more fully below, the significant money laundering or terrorist financing risk associated with the operation of a credit card system sought to be minimized by this interim final rule is the operator's authorization or licensing of issuing or acquiring institutions without conducting appropriate due diligence relating to the money laundering or terrorist financing risk posed by those institutions. A merchant or a vendor that issues its own card does not present that particular risk because it does not perform that function.[6]

[5] Banks issuing merchant or vendor cards are already subject to anti-money laundering regulation enforced by the bank regulators.

[6] This interim final rule neither considers nor addresses the money laundering or terrorist financing risks associated with issuing institutions. However, this should not be construed to suggest no such risks exist.

With general purpose credit cards, the operator of a credit card system plays a vital role in the authorization, clearance, and settlement of credit card purchases. This role is important to understanding both how the operator of the credit card system can assist in preventing money laundering or terrorist financing, as well as the practical limitations placed on the operator in this regard. Authorization is the process by which the issuer of the credit card approves or rejects a purchase at the time the cardholder seeks to access the line of credit associated with the card. Typically, the merchant swipes the credit card through a terminal that electronically captures the relevant data.[7] Once the merchant keys in the amount of the purchase, that information is transmitted electronically through the operator's system to the issuing bank for approval. If appropriate, the purchase is approved. Once approved, the transaction with the consumer is consummated.

The next step is the clearance process. The merchant submits the credit card payment information to its merchant bank for payment. The merchant bank credits the merchant's account, and submits the purchase information to the operator of the credit card system. The operator then sends the purchase information to the issuing bank for payment.

The final step is the settlement process. The issuing bank transmits the funds owed by virtue of the purchase to the operator of the credit card system. The operator then transmits the funds to the merchant bank in settlement of the debt. In the settlement process, funds are transmitted through traditional payment systems. The issuing bank then bills the cardholder for the transaction in accordance with the credit agreement.

Thus, the operator of the credit card system not only controls which entities may issue or process transactions involving its card, but it also serves as a clearinghouse where debts are

[7] "Electronic Data Capture (EDC) is a point-of-sale terminal that reads the information embedded in the magnetic strip of bank cards. These terminals electronically authorize and capture transaction data, thus eliminating the need

settled and from which payments are made and received. This is the functional definition of an operator of a credit card system. The reality is that there are few operators of credit card systems in the United States, certainly in contrast to the number of issuing and acquiring banks.

In addition, a debit card may at times also be used as a credit card. A debit card generally accesses an existing deposit account at an insured depository institution from which funds are withdrawn upon use of the debit card. Debit cards generally require the use of a personal identification number at the point of sale. Some debit cards can also function as a credit card and some credit card system operators also authorize, clear, and settle debit card transactions. Often such dual use cards are marked with a logo or insignia of the operator of the credit card system. The interim final rule applies to both functions of a dual use card.[8]

B. The Authorization of Acquiring and Issuing Banks

The success of a general purpose credit card depends upon its availability to consumers and the extent to which it is widely accepted by merchants and vendors. The operator of the system is directly responsible for selecting and approving issuing and acquiring institutions to become a part of the system, and setting the rules by which they must abide. In addition, in its role of ensuring that the member institutions continue to abide by the membership rules, the operator of the system indirectly plays a role in selecting and approving other users in the system, including cardholders and merchants. These functions—determining which institutions may serve as issuing or acquiring institutions, and setting and ensuring ongoing compliance with the system's rules and regulations—play a crucial role in determining the extent to which a credit card system may be vulnerable to money laundering or terrorist financing.

---

for a paper deposit." The 1997 GAO Report at 108.

[8] While this interim final rule applies to the debit card functions performed by an operator of a credit card system accepting dual use cards, the rule does not apply generally to operators of a debit card system. Treasury intends to

It appears that during the authorization, clearance, and settlement process, cardholder and individual merchant names may not be transmitted through the operator's credit card system.[9] Comprehensive cardholder information is maintained by the issuing institutions. Similarly, information about the merchants that accept the card is maintained by the acquiring institutions. Thus, many important anti-money laundering functions of necessity reside with the issuing and acquiring institutions, and, in the United States, existing anti-money laundering regulations typically govern these institutions. However, the initial and continuing authorization of institutions to issue a credit card and process credit card transactions is within the sole control of the operator of the credit card system.

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

Incentives exist for the operator of a credit card system to minimize financial losses caused by fraud in connection with the use of its credit card. According to the industry, those incentives encourage operators to scrutinize institutions seeking authorization to become issuers or acquirers to ensure that member institutions themselves do not pose an unreasonable risk of loss, whether through participation in fraud or through their issuing or acquiring functions. This interim final 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.

Operators of credit card systems support the efforts of issuing and acquiring institutions in the detection of fraudulent uses of their credit cards. Some of the methods for identifying irregular and possibly fraudulent transactions are quite sophisticated. For example, operators and

---

consider whether operators of debit card systems should likewise be included as financial institutions under the BSA and thus be subject to the anti-money laundering program requirement.

some issuers use computers to flag potentially fraudulent uses of credit cards as the purchases are authorized, cleared, and settled by comparing recent purchases with the cardholder's purchase history as well as known typologies of fraudulent uses. At this time, Treasury does not necessarily intend to require operators of credit card systems, as part of their anti-money laundering program, to use this type of fraud detection capabilities to detect potential money laundering or terrorist financing. The reason is practical—it is not clear that potential money laundering or terrorist financing can be easily identified with the current technology that evaluates transactions passing through the operator's system. However, Treasury hopes to work with operators of credit card systems going forward to develop, where possible, typologies of money laundering or terrorist financing that may be capable of being identified through existing fraud detection mechanisms.[10]

D. Money Laundering and Terrorist Financing Risks Associated with Credit Cards from the Perspective of the Operator of a Credit Card System

Once in the hands of a consumer, a general purpose credit card is designed to facilitate the purchase of goods or services or the securing of cash advances worldwide with minimal delay. But the very attributes that make credit cards attractive to legitimate consumers are the attributes that make them susceptible to potential abuse. The myriad ways in which credit cards may be abused for money laundering or terrorist financing are beyond the scope of this preamble.[11] Instead, the primary focus of this interim final rule is on the risks—and the need to minimize them—associated with the operator authorizing, and maintaining authorization for, issuing and acquiring institutions.

---

[9] Operators may well have complete information regarding cardholders and merchants during the authorization and settlement process, *e.g.*, if the operator also serves as an issuer.

[10] FinCEN, in conjunction with the Bank Secrecy Act Advisory Group, publishes an annual SAR Activity Review that discusses typologies revealed in SAR filings.

[11] The GAO is currently drafting a report that will analyze money laundering in the credit card industry.

Absent effective anti-money laundering controls in issuing and acquiring institutions, the use of a credit card may provide a convenient way for money launderers or those financing terrorism to access their tainted funds all over the world. For example, if a foreign bank lacking adequate anti-money laundering controls is authorized to issue a credit card capable of being used in the United States, there exists an increased risk that illicit funds located in the foreign bank may be accessed—and those funds injected into the U.S. financial system—by account holders using the credit card in the United States to make purchases, obtain cash advances, or, if it is a dual use card, use the card as a debit card. The problem is exacerbated by the fact that the operator of the credit card system that clears and settles transactions might not have information about the identity of the cardholder or the source of funds used to pay the debts at the time the transactions are processed.

Under the Act, and even prior to the Act, numerous restrictions and heightened due diligence requirements were placed on U.S. banks and securities brokers and dealers maintaining accounts for certain types of foreign banks and foreign banks located in jurisdictions identified as lacking adequate anti-money laundering controls and supervision. In this way, the Act seeks to eliminate or minimize known risks to the U.S. financial system, even requiring the termination of accounts for certain financial institutions when the risk is deemed too high. Examples of known risks identified by the Act include maintaining "correspondent accounts" for: (1) foreign banks located in jurisdictions identified as lacking basic anti-money laundering controls; (2) foreign shell banks, that is, banks with no physical presence in any jurisdiction; and (3) foreign banks operating under an offshore banking license.[12]

[12] *See* Act sections 312 and 313; *see also* MINORITY STAFF OF THE SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS, 107TH CONG., CORRESPONDENT BANKING: A GATEWAY FOR MONEY LAUNDERING, 14-18 (S. Prt. 2001). Congress defined a "correspondent account" broadly in the Act to include any "account established to receive deposits from, make payments on behalf of a foreign financial institution, or handle other financial

Despite the risks associated with these identified foreign financial institutions, the prohibitions or enhanced due diligence obligations have not been applied directly to operators of credit card systems that may well authorize foreign financial institutions to issue their credit cards and access their systems. But if such foreign banks were authorized to issue credit cards capable of being used in the United States, customers of such banks would have the opportunity to inject illicit funds into the U.S. financial system.

Recent examples confirm the potential for utilizing a credit card system to access in the United States funds located in a foreign financial institutions. The Internal Revenue Service has successfully sought permission to serve "John Doe" subpoenas on MasterCard International, American Express Travel Related Services Co., and VISA International seeking records relating to U.S. citizens with credit, charge, and debit cards issued by banks or other financial institutions located in identified tax havens. According to the IRS, U.S. citizens are using credit, charge, and debit cards to access in the United States funds placed in these foreign banks and financial institutions to avoid U.S. taxes. The tax haven jurisdictions do not disclose account information to the United States for purposes of enforcing U.S. tax laws. If credit cards can be used to access funds located in tax havens to avoid U.S. income tax obligations, credit cards have the potential to be used to access illicit funds located in money laundering havens if banks in those jurisdictions are given permission by the operator of the credit card system to issue the credit cards. The same principle holds true for illicit funds deposited in U.S. financial institutions that issue credit cards. To the extent the issuing institution lacks sufficient anti-money laundering controls, issuance of a credit card would allow easy and seemingly "clean" access to tainted funds.

---

transactions related to such institution." Act section 311 (31 U.S.C. 5318A(e)(1)(B)). Treasury is now considering comments received on a previous proposed rule in which the statutory definition was adopted without limitation.

E. The Anti-Money Laundering Program

As the foregoing discussion demonstrates, the anti-money laundering program required by this interim final 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. Such 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. The anti-money laundering program must also have procedures to minimize the opportunity for money laundering or terrorist financing when identified high-risk institutions are issuing or acquiring institutions. In fulfilling obligations under the interim final rule, it is expected that operators will tailor existing rules and guidelines governing member institutions to minimize the risk of money laundering or terrorist financing. Finally, 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 interim final rule is meant to provide guidance to operators on identified risks.

The focus of the rule is on what operators can and do control, and it may be that most are already taking the steps outlined in this rule. The interim final 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.

See 66 Fed. Reg. 67,460 (Dec. 28, 2001) (implementing sections 313 and 319(b) of the Act).

Finally, in addition to compliance with mandatory regulatory requirements, Treasury and FinCEN encourage operators of credit card systems to have procedures for voluntarily reporting suspected terrorist activity to FinCEN using its Financial Institutions Hotline (1-866-556-3974).

II. Section-by-Section Analysis

A. Section 103.135(a)—Definitions

The definition of an operator of a credit card system is a functional one. It includes any entity that (1) operates a system that clears and settles transactions involving its credit card; and (2) authorizes another entity to serve as an issuing or acquiring institution for the operator's credit card. The credit card must be capable of being used in the United States. An operator may be a bank, a consortium or association of banks, or any other entity performing the functions described. All operators of credit card systems doing business in the United States are covered by the interim final rule.

Issuing and acquiring institutions within such systems need not be located in the United States and may be foreign entities. An issuing institution is any entity authorized by the operator to issue the operator's credit card. An acquiring institution is any entity authorized by the operator to contract with merchants to process transactions involving the operator's credit card. The interim final rule adopts the definition of a credit card found in the Truth in Lending Act, a definition that includes charge cards. Finally, debit cards capable of being used as a credit card are covered by this interim final rule.

B. Section 103.135(b) and (c)—The Required Anti-Money Laundering Program

Section 103.135(b) requires that each operator of a credit card system have an anti-money laundering program reasonably designed to prevent the system from being used to launder money or to finance terrorist activities. The program must be in writing and approved by senior

management. The minimum requirements for the anti-money laundering program are set forth in section 103.135(c). Beyond these minimum requirements, however, the anti-money laundering program is designed to give operators of a credit card system flexibility to design their programs to meet the specific risks presented. The steps necessary to guard against an institution, foreign or domestic, issuing or processing transactions involving the credit card in connection with money laundering when the institution does not fall within a high risk category may be minimal if the institution and its anti-money laundering controls are well known to the operator. The fact that a member institution is a foreign bank or entity is not itself determinative of the risk posed.

The minimum standards for the anti-money laundering program set forth in this interim final rule become effective July 24, 2002.

1. Section 103.135(c)(1)—Policies, Procedures and Internal Controls

Section 103.135(c)(1) requires the operator's anti-money laundering program to include policies, procedures and internal controls focused on the process of authorizing and maintaining authorization for issuing and acquiring institutions. This provision will thus involve the operator tailoring existing anti-fraud and risk of loss assessment procedures to ensure that money laundering and terrorist financing risks are taken into account. It will further 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. Finally, the interim final rule makes clear that this obligation is ongoing. The frequency with which banks or entities are reviewed to ensure compliance with required procedures will depend upon the operator's assessment of the risk posed by the particular bank or entity.

It is anticipated that the type of information to be considered by the operator in evaluating the risks of money laundering or terrorist financing posed by an issuing or acquiring institution will include many of the same factors that bear on whether the institution represents a risk of fraud or insolvency. In addition, the operator must consider information concerning the institutions, the jurisdictions in which they are located or licensed, and any other money laundering or terrorist financing information provided by Treasury, FinCEN, and other U.S. government sources. Information in publicly available sources should be considered as well. In some situations, information relevant to anti-money laundering controls or risks may need to be obtained from the institution itself, *e.g.*, information relating to the institution's anti-money laundering controls. If an operator is unable to obtain sufficient information from existing or potential issuing or acquiring institutions, this must be taken into account in evaluating the overall money laundering or terrorist financing risk.

For the purpose of making the risk assessment required by section 103.135(c)(1)(i), section 103.135(c)(1)(ii) sets forth the presumption that certain categories of foreign banks or other institutions pose an increased, or in some cases an unreasonable, risk of money laundering or terrorist financing. Accordingly, an operator's anti-money laundering program must be designed to ensure that the institutions identified under this paragraph, if they are permitted to serve as issuing or acquiring institutions, have received a thorough assessment of the risk of money laundering or terrorist financing that they pose in connection with the issuance or acceptance of the operator's credit card. Additionally, the anti-money laundering program must also ensure that the operator has taken reasonable steps to minimize the risks associated with such institutions.

Within this collection of high risk institutions, even though there is a presumption of a heightened risk, operators still retain the flexibility to assess the risk posed in each case to determine whether and under what conditions such an institution may serve as an issuing or acquiring institution. Some of the categories of institutions within this paragraph have been effectively cut off from the U.S. financial system, *e.g.*, foreign shell banks that are not regulated affiliates. Given the unreasonable risk that funds located in such financial institutions are derived from the proceeds of illegal activities or directly support terrorism, there is a significantly heightened risk that allowing them to issue a credit card will introduce the illicit funds into the U.S. financial system. In such cases, the steps necessary to guard against money laundering or terrorist financing by such institutions in connection with the operator's credit card will be comprehensive. On the other hand, other institutions within this list may, upon examination, pose a less significant risk of money laundering or terrorist financing. As a result, the reasonable steps to be taken by the operator to guard against money laundering or terrorist financing will be reduced.

As with all issuing and acquiring institutions, the obligation to assess money laundering and terrorist financing risks applies to both prospective and existing issuing or acquiring institutions. However, institutions falling within the categories identified in section 103.135(c)(1)(ii), because they pose greater risks, should be reviewed by the operator with greater frequency.

By identifying certain high risk institutions, we do not intend to imply that no other institutions pose similar risks. To the contrary, it is incumbent upon the operator to ensure that its anti-money laundering program will identify other institutions posing similar risks.

Section 103.135(c)(1)(iii) confirms that operators of a credit card system must ensure the operators' compliance with any applicable provisions of the BSA or the implementing regulations. At this time, the only BSA provision applicable to an operator of a credit card system, with the exception of this interim final rule, is the obligation to report on Form 8300 the receipt of cash or certain monetary instruments totaling more than $10,000 in one transaction or two or more transactions. Given the functions performed by the operator of a credit card system, it seems unlikely that cash or cash equivalents will be received. However, this provision is inserted in the interim final rule in the event future BSA requirements are imposed on operators of credit card systems.

2. Sections 103.135(c)(2)-(4)—The Compliance Officer, Employee Training, and the Independent Assessment

In connection with its anti-money laundering program, the operator of a credit card system must designate a person or persons to be responsible for administering the anti-money laundering program. The person or persons should be competent and knowledgeable regarding BSA requirements and money laundering issues and risks, and be empowered with full responsibility and authority to develop and enforce appropriate policies and procedures. The role of the compliance officer is to ensure that (1) the program is implemented; (2) appropriate due diligence is being conducted on existing and potential issuers and acquirers in accordance with the requirements of this interim final rule; and (3) the program is updated to reflect new directives from Treasury or FinCEN. The compliance officer is also responsible for ensuring that appropriate personnel are trained and educated in accordance with section 103.135(c)(3).

Employee training is an integral part of any anti-money laundering program. Those employees with responsibility under the program must be trained in the requirements of this rule and money laundering risks generally so that "red flags" associated with existing or potential

issuing or acquiring institutions can be identified. Such training could be conducted by outside or in-house seminars, and could include computer-based training. The nature, scope, and frequency of the education and training program of the operator will depend upon the functions performed. However, those with obligations under the anti-money laundering program must be sufficiently trained to carry out their responsibilities effectively. Moreover, these employees should receive periodic updates and refreshers regarding the anti-money laundering program.

Finally, the program must provide for an independent audit of the program on a periodic basis to ensure that it complies with this interim final rule and that it functions as designed. Although the interim final rule refers to an audit, the term does not equate with a financial audit and need not be performed by an outside consultant or accountant. The independent audit may be performed by an employee of the operator, so long as the auditor is not the compliance officer or others involved in administering the program. The frequency of the independent audit will depend upon the operator's assessment of the risks posed. The audit should be accompanied by a written assessment or report, and any recommendations resulting from such review should be implemented promptly or reviewed by senior management.

III. Administrative Procedure Act

The provisions of 31 U.S.C. 5318(h)(1), requiring all financial institutions to establish anti-money laundering programs with at least four identified elements, become effective April 24, 2002. This interim rule provides guidance to operators of credit card systems on how to comply with the law in effect on that date and does not impose any obligation on any financial institution that is not required by section 352 of the Act. Accordingly, good cause is found to dispense with notice and public procedure as unnecessary pursuant to 5 U.S.C. 553(b)(B), and to

make the provisions of the interim rule effective in less than 30 days pursuant to 5 U.S.C. 553(d)(1) and (3).

VI. Paperwork Reduction Act.

This regulation is being issued without prior notice and public procedure pursuant to the Administrative Procedure Act (5 U.S.C. 553). For this reason, the collection of information contained in this interim final rule has been reviewed under the requirements of the Paperwork Reduction Act (44 U.S.C. 3507(j)) and, pending receipt and evaluation of public comments, approved by the Office of Management and Budget (OMB) under control number 1506-0020. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid control number assigned by OMB.

The collection of information in this interim final rule is in 31 CFR 103.135(b). The information will be used by federal agencies to verify compliance by operators of credit card systems with the provisions of 31 CFR 103.135. The collection of information is mandatory. The likely recordkeepers are businesses.

In accordance with the requirements of the Paperwork Reduction Act of 1995, 44 U.S.C. 3506(c)(2)(A), and its implementing regulations, 5 CFR 1320, the following information concerning the collection of information as required by 31 CFR 103.135(b) is presented to assist those persons wishing to comment on the information collection.

Description of Recordkeepers: Operators of Credit Card Systems, as defined in 31 CFR 103.135(a).

Estimated Number of Recordkeepers: 6.

Estimated Average Annual Burden Hours Per Recordkeeper: The estimated average burden associated with the collection of information in this interim final rule is 1 hour per recordkeeper.

Estimated Total Annual Recordkeeping Burden: 6 hours.

Comments concerning the collection of information should be sent to the Office of Management and Budget, Attn: Alexander T. Hunt, Office of Information and Regulatory Affairs, Office of Management and Budget, New Executive Office Building, Room 3208, Washington, DC 20503, with copies to FinCEN at Department of the Treasury, Financial Crimes Enforcement Network, Post Office Box 39, Vienna, Virginia, 22183.

FinCEN specifically invites comments on the following subjects: (a) whether the collection of information is necessary for the proper performance of the mission of FinCEN, including whether the information shall have practical utility; (b) the accuracy of FinCEN's estimate of the burden of the collection of information; (c) ways to enhance the quality, utility, and clarity of the information to be collected; (d) ways to minimize the burden of the collection of information on respondents, including through the use of automated collection techniques or other forms of information technology; and (e) estimates of capital or start-up costs and costs of operation, maintenance, and purchase of services to provide information.

V. Regulatory Flexibility Act

Because no notice of proposed rulemaking is required for this interim final rule, the provisions of the Regulatory Flexibility Act (5 U.S.C. 601 et seq.) do not apply.

VI. Executive Order 12866

This interim final rule is not a "significant regulatory action" as defined in Executive Order 12866. Accordingly, a regulatory assessment is not required.

List of Subjects in 31 CFR Part 103

Banks, banking, Brokers, Counter money laundering, Counter-terrorism, Currency, Foreign banking, Reporting and recordkeeping requirements.

PART 103 – FINANCIAL RECORDKEEPING AND REPORTING OF CURRENCY AND FOREIGN TRANSACTIONS

1. The authority citation for part 103 continues to read as follows:

Authority: 12 U.S.C. 1829b and 1951-1959; 31 U.S.C. 5311-5331; title III, secs. 314, 352, Pub. L. 107-56, 115 Stat. 307.

2. In subpart I, add new §103.135 to read as follows:

§103.135 Anti-money laundering programs for operators of credit card systems.

(a) *Definitions*. For purposes of this section:

(1) *Operator of a credit card system* means any person doing business in the United States that operates a system for clearing and settling transactions in which the operator's credit card, whether acting as a credit or debit card, is used to purchase goods or services or to obtain a cash advance. To fall within this definition, the operator must also have authorized another person (whether located in the United States or not) to be an issuing or acquiring institution for the operator's credit card.

(2) *Issuing institution* means a person authorized by the operator of a credit card system to issue the operator's credit card.

(3) *Acquiring institution* means a person authorized by the operator of a credit card system to contract, directly or indirectly, with merchants or other persons to process transactions, including cash advances, involving the operator's credit card.

(4) *Operator's credit card* means a credit card capable of being used in the United States that:

(i) Has been issued by an issuing institution; and

(ii) Can be used in the operator's credit card system.

(5) *Credit card* has the same meaning as in 15 U.S.C. 1602(k). It includes charge cards as defined in 12 CFR 226.2(15).

(6) *Foreign bank* means any organization that is organized under the laws of a foreign country; engages in the business of banking; is recognized as a bank by the bank supervisory or monetary authority of the country of its organization or the country of its principal banking operations; and receives deposits in the regular course of its business. For purposes of this definition:

(i) The term foreign bank includes a branch of a foreign bank in a territory of the United States, Puerto Rico, Guam, American Samoa, or the U.S. Virgin Islands.

(ii) The term foreign bank does not include:

(A) A U.S. agency or branch of a foreign bank; and

(B) An insured bank organized under the laws of a territory of the United States, Puerto Rico, Guam, American Samoa, or the U.S. Virgin Islands.

(b) *Anti-money laundering program requirement*. Effective July 24, 2002, each operator of a credit card system shall develop and implement a written anti-money laundering program reasonably designed to prevent the operator of a credit card system from being used to facilitate money laundering and the financing of terrorist activities. The program must be approved by senior management. Operators of credit card systems must make their anti-money laundering programs available to the Department of the Treasury or the appropriate Federal regulator for review.

(c) *Minimum requirements.* At a minimum, the program must:

(1) Incorporate policies, procedures, and internal controls designed to ensure the following:

(i) That the operator does not authorize, or maintain authorization for, any person to serve as an issuing or acquiring institution without the operator taking appropriate steps, based upon the operator's money laundering or terrorist financing risk assessment, to guard against that person issuing the operator's credit card or acquiring merchants who accept the operator's credit card in circumstances that facilitate money laundering or the financing of terrorist activities;

(ii) For purposes of making the risk assessment required by paragraph (c)(1)(i) of this section, the following persons are presumed to pose a heightened risk of money laundering or terrorist financing when evaluating whether and under what circumstances to authorize, or to maintain authorization for, any such person to serve as an issuing or acquiring institution:

(A) A foreign shell bank that is not a regulated affiliate, as those terms are defined in 31 CFR 104.10(e) and (j);

(B) A person appearing on the Specially Designated Nationals List issued by Treasury's Office of Foreign Assets Control;

(C) A person located in, or operating under a license issued by, a jurisdiction whose government has been identified by the Department of State as a sponsor of international terrorism under 22 U.S.C. 2371;

(D) A foreign bank operating under an offshore banking license, other than a branch of a foreign bank if such foreign bank has been found by the Board of Governors of the Federal Reserve System under the Bank Holding Company Act (12 U.S.C. 1841, et seq.) or the International Banking Act (12 U.S.C. 3101, et seq.) to be subject to comprehensive supervision or regulation on a consolidated basis by the relevant supervisors in that jurisdiction;

(E) A person located in, or operating under a license issued by, a jurisdiction that has been designated as noncooperative with international anti-money laundering principles or

procedures by an intergovernmental group or organization of which the United States is a member, with which designation the United States representative to the group or organization concurs; and

(F) A person located in, or operating under a license issued by, a jurisdiction that has been designated by the Secretary of the Treasury pursuant to 31 U.S.C. 5318A as warranting special measures due to money laundering concerns;

(iii) That the operator is in compliance with all applicable provisions of subchapter II of chapter 53 of title 31, United States Code and this part;

(2) Designate a compliance officer who will be responsible for assuring that:

(i) The anti-money laundering program is implemented effectively;

(ii) The anti-money laundering program is updated as necessary to reflect changes in risk factors or the risk assessment, current requirements of part 103, and further guidance issued by the Department of the Treasury; and

(iii) Appropriate personnel are trained in accordance with paragraph (c)(3) of this section;

(3) Provide for education and training of appropriate personnel concerning their responsibilities under the program; and

(4) Provide for an independent audit to monitor and maintain an adequate program. The scope and frequency of the audit shall be commensurate with the risks posed by the persons authorized to issue or accept the operator's credit card. Such audit may be conducted by an officer or employee of the operator, so long as the reviewer is not the person designated in paragraph (c)(2) of this section or a person involved in the operation of the program.

Dated: _____

_____
James F. Sloan
Director, Financial Crimes Enforcement Network