[67 FR 9877, Mar. 4, 2002]

APPENDIX C TO PART 103—INTERPRETIVE RULES

RELEASE NO. 2004–01

This Interpretive Guidance sets forth our interpretation of the regulation requiring Money Services Businesses that are required to register with FinCEN to establish and maintain anti-money laundering programs. See 31 CFR 103.125. Specifically, this Interpretive Guidance clarifies that the anti-money laundering program regulation requires Money Services Businesses to establish adequate and appropriate policies, procedures, and controls commensurate with the risks of money laundering and the financing of terrorism posed by their relationship with foreign agents or foreign counterparties of the Money Services Business.[1]

Under existing Bank Secrecy Act regulations, we have defined Money Services Businesses to include five distinct types of financial services providers and the U.S. Postal Service: (1) Currency dealers or exchangers; (2) check cashers; (3) issuers of traveler's checks, money orders, or stored value; (4) sellers or redeemers of traveler's checks, money orders, or stored value; and (5) money transmitters. See 31 CFR 103.11(uu). With limited exception, Money Services Businesses are subject to the full range of Bank Secrecy Act regulatory controls, including the anti-money laundering program rule, suspicious activity and currency transaction reporting rules, and various other identification and recordkeeping rules.[2]

Many Money Services Businesses, including the vast majority of money transmitters in the United States, operate through a system of agents both domestically and internationally. We estimate that a substantial majority of all cross-border remittances by money transmitters are conducted using this model. Other Money Services Businesses may operate through more informal relationships, such as the trust-based hawala system.[3] Regardless of the form of the relationship between a Money Services Business and its foreign agents or counterparties, Money Services Business transactions generally are initiated by customers seeking to send or receive funds, cash checks, buy or sell money orders or traveler's checks, or buy or sell currency. The customer directs the Money Services Business to execute the transactions; the Money Services Business does not unilaterally determine the recipient of its products or services. Although the customer can use the Money Services Business' services, the customer does not typically establish an account relationship with the Money Services Business. The focus of this Interpretive Guidance is the establishment of, and ongoing relationship between, a Money Services Business and its foreign agent or foreign counterparty that facilitates the flow of funds cross-border into and out of the United States on behalf of customers.

THE CROSS-BORDER FLOW OF FUNDS THROUGH MONEY SERVICES BUSINESSES AND ASSOCIATED RISKS

Ensuring that financial institutions based in the United States establish and apply adequate and appropriate policies, procedures, and controls in their anti-money laundering compliance programs to protect the international gateways to the U.S. financial system is an essential element of the Bank Secrecy Act regulatory regime. This Interpretive Guidance forms a part of our comprehensive approach to accomplishing this

[1] This Interpretive Guidance focuses on the need to control risks arising out of the relationship between a Money Service Business and its foreign counterparty or agent. Under existing FinCEN regulations, only Money Service Business principals are required to register with FinCEN, and only Money Service Business principals establish the counterparty or agency relationships. 31 CFR 103.41. Accordingly, this Interpretive Guidance only applies to those Money Service Businesses required to register with FinCEN, that is, only those Money Service Businesses that may have a relationship with a foreign agent or counterparty.

[2] *See* 31 CFR 103.125 (requirement for Money Service Businesses to establish and maintain an anti-money laundering compliance program); 31 CFR 103.22 (requirement for Money Service Businesses to file currency transaction reports); 31 CFR 103.20 (requirement for Money Service Businesses, other than check cashers and issuers, sellers, or redeemers of stored value, to file suspicious activity reports); 31 CFR 103.29 (requirement for Money Service Businesses that sell money orders, traveler's checks, or other instruments for cash to verify the identity of the customer and create and maintain a record of each cash purchase between $3,000 and $10,000, inclusive); 31 CFR 103.33(f) (requirement for Money Service Businesses that send or accept instructions to transmit funds of $3,000 or more to verify the identity of the sender or receiver and create and maintain a record of the transmittal regardless of the method of payment); and 31 CFR 103.37 (requirement for currency exchangers to create and maintain a record of each exchange of currency in excess of $1,000).

[3] For an analysis of informal value transfer systems, see FinCEN's Report to Congress Pursuant to Section 359 of the Patriot Act, available on *www.fincen.gov*.

goal. To the extent Money Services Businesses utilize relationships with foreign agents or counterparties to facilitate the movement of funds into or out of the United States, they must take reasonable steps to guard against the flow of illicit funds, or the flow of funds from legitimate sources to persons seeking to use those funds for illicit purposes, through such relationships.

The money laundering or terrorism financing risks associated with foreign agents or counterparties are similar to the risks presented by domestic agents of Money Services Businesses. For example, the foreign agent of the domestic Money Services Business may have lax anti-money laundering policies, procedures, and internal controls, or actually may be complicit with those seeking to move illicit funds. In some instances, the risk with foreign agents can be greater than with domestic agents because foreign agents are not subject to the Bank Secrecy Act regulatory regime; the extent to which they are subject to anti-money laundering regulation, and the quality of that regulation, will vary with the jurisdictions in which they are located.

There are a variety of ways in which a Money Services Business may be susceptible to the unwitting facilitation of money laundering through foreign agents or counterparties. For example, our review of Bank Secrecy Act data revealed several instances of suspected criminal activity—detected by existing anti-money laundering and suspicious activity reporting programs of Money Services Businesses and banks—where foreign agents of Money Services Business have engaged in bulk sales of sequentially numbered, U.S. denominated traveler's checks or blocks of money orders, to one or two individuals. The individuals involved frequently purchased the instruments on multiple dates and in different locations, structuring the purchases to avoid reporting thresholds and issuer limits on daily instrument sales. The instruments usually had illegible signatures or failed to designate a beneficiary or payor. The instruments were then negotiated with one or more dealers in goods, such as diamonds, gems, or precious metals, deposited in foreign banks, and cleared through U.S. banks. In such cases, the clearing banks were so far removed from the transactions that they could not trace back or screen either the intervening transactions or the individuals involved in the transactions.

A case involving suspicious activity in a Money Services Business' domestic agent provides a further example of the type of high-risk activity that also may be engaged in by foreign agents or counterparties. In this instance, the domestic Money Service Business had policies, procedures, and controls that facilitated the detection of illicit activity at the agent. A group of six customers entered a money transmitter agent at approximately five-minute intervals to send the same structured amounts ($2,500) to the same receiver in a foreign country. Several weeks later, another group of six customers entered the same agent location and conducted an identical pattern of successive $2,500 transfers (a few minutes apart) to the same recipient in the same foreign country as the first set of transactions. Some of the individuals in the second group had the same last names as customers in the first group. Additional suspicious activity reports filed by the primary Money Services Business identified several other groups of customers initiating money transfers at this same agent business location, in the same manner, and in the same overall time frame. This activity by an agent drew the scrutiny of the Money Services Business, and in addition to the filing of suspicious activity reports, led to the termination of the relationship of the Money Services Business with the agent.

These examples of illicit activity occurring at the agents of Money Services Businesses underscore the need for Money Services Businesses to include, as a part of their anti-money laundering programs, procedures, policies, and controls to govern relationships with foreign agents and counterparties to enable the Money Services Business to perform the appropriate level of suspicious activity and risk monitoring. We believe that this obligation is an essential part of each Money Services Business' existing obligation under 31 CFR 103.125 to develop and implement an effective anti-money laundering program.[4] This Interpretive Guidance will aid Money Services Businesses in adopting appropriate risk-based policies, procedures, and controls on cross-border relationships with foreign agents and counterparties.

ANTI-MONEY LAUNDERING PROGRAM ELEMENTS RELATING TO FOREIGN AGENTS AND COUNTERPARTIES

Under 31 CFR 103.125(a), Money Services Businesses are required to develop, implement, and maintain an effective anti-money laundering program reasonably designed to prevent the Money Services Business from being used to facilitate money laundering and the financing of terrorist activities. The program must be commensurate with the risks posed by the location, size, nature, and volume of the financial services provided by the Money Services Business. Additionally, the program must incorporate policies, procedures, and controls reasonably designed to

[4] FinCEN previously interpreted 31 CFR 103.125 to impose a similar obligation on a money transmitter with respect to its domestic agents. See Matter of Western Union, No. 2003–2 (Mar. 6, 2003) (*www.fincen.gov*).

assure compliance with the Bank Secrecy Act and implementing regulations.

With respect to Money Services Businesses that utilize foreign agents or counterparties, a Money Services Business' anti-money laundering program must include risk-based policies, procedures, and controls designed to identify and minimize money laundering and terrorist financing risks associated with foreign agents and counterparties that facilitate the flow of funds into and out of the United States. The program must be aimed at preventing the products and services of the Money Services Business from being used to facilitate money laundering or terrorist financing through these relationships and detecting the use of these products and services for money laundering or terrorist financing by the Money Services Business or agent. Relevant risk factors may include, but are not limited to:

• The foreign agent or counterparty's location and jurisdiction of organization, chartering, or licensing. This would include considering the extent to which the relevant jurisdiction is internationally recognized as presenting a greater risk for money laundering or is considered to have more robust anti-money laundering standards.

• The ownership of the foreign agent or counterparty. This includes whether the owners are known, upon reasonable inquiry, to be associated with criminal conduct or terrorism. For example, have the individuals been designated by Treasury's Office of Foreign Assets Control as Specially Designated Nationals or Blocked Persons (*i.e.*, involvement in terrorism, drug trafficking, or the proliferation of weapons of mass destruction)?

• The extent to which the foreign agent or counterparty is subject to anti-money laundering requirements in its jurisdiction and whether it has established such controls.

• Any information known or readily available to the Money Services Business about the foreign agent or counterparty's anti-money laundering record, including public information in industry guides, periodicals, and major publications.

• The nature of the foreign agent or counterparty's business, the markets it serves, and the extent to which its business and the markets it serves present an increased risk for money laundering or terrorist financing.

• The types and purpose of services to be provided to, and anticipated activity with, the foreign agent or counterparty.

• The nature and duration of the Money Services Business' relationship with the foreign agent or counterparty.

Specifically, a Money Services Business' anti-money laundering program should include procedures for the following:

1. Conduct of Due Diligence on Foreign Agents and Counterparties

Money Services Businesses should establish procedures for conducting reasonable, risk-based due diligence on potential and existing foreign agents and counterparties to help ensure that such foreign agents and counterparties are not themselves complicit in illegal activity involving the Money Services Business' products and services, and that they have in place appropriate anti-money laundering controls to guard against the abuse of the Money Services Business' products and services. Such due diligence must, at a minimum, include reasonable procedures to identify the owners of the Money Services Business' foreign agents and counterparties, as well as to evaluate, on an ongoing basis, the operations of those foreign agents and counterparties and their implementation of policies, procedures, and controls reasonably designed to help assure that the Money Services Business' products and services are not subject to abuse by the foreign agent's or counterparty's customers, employees, or contractors.[5] The extent of the due diligence required will depend on a variety of factors specific to each agent or counterparty. We expect Money Services Businesses to assess such risks and perform due diligence in a manner consistent with that risk, in light of the availability of information.

2. Risk-based Monitoring of Foreign Agents or Counterparties

In addition to the due diligence described above, in order to detect and report suspected money laundering or terrorist financing, Money Services Businesses should establish procedures for risk-based monitoring and review of transactions from, to, or through the United States that are conducted through foreign agents and counterparties.[6] Such procedures should also

[5] Our anti-money laundering program rule, 31 CFR 103.125(d)(iii), permits Money Service Businesses to satisfy this last requirement with regard to their domestic agents (which are also Money Service Businesses under the BSA regulations), by allocating responsibility for the program to their agents. Such an allocation, however, does not relieve a Money Service Business from ultimate responsibility for establishing and maintaining an effective anti-money laundering program. *Id.*

[6] Nothing in this Interpretive Guidance is intended to require Money Service Businesses to monitor or review, for purposes of the Bank Secrecy Act, transactions or activities of foreign agents or counterparties that occur entirely outside of the United States and do not flow from, to, or through the United States.

focus on identifying material changes in the agent's risk profile, such as a change in ownership, business, or the regulatory scrutiny to which it is subject.

The review of transactions should enable the Money Services Business to identify and, where appropriate, report as suspicious such occurrences as: instances of unusual wire activity, bulk sales or purchases of sequentially numbered instruments, multiple purchases or sales that appear to be structured, and illegible or missing customer information. Additionally, Money Services Businesses should establish procedures to assure that their foreign agents or counterparties are effectively implementing an anti-money laundering program and to discern obvious breakdowns in the implementation of the program by the foreign agent or counterparty.

Similarly, money transmitters should have procedures in place to enable them to review foreign agent or counterparty activity for signs of structuring or unnecessarily complex transmissions through multiple jurisdictions that may be indicative of layering. Such procedures should also enable them to discern attempts to evade identification or other requirements, whether imposed by applicable law or by the Money Services Business' own internal policies. Activity by agents or counterparties that appears aimed at evading the Money Services Business' own controls can be indicative of complicity in illicit conduct; this activity must be scrutinized, reported as appropriate, and corrective action taken as warranted.

3. Corrective Action and Termination

Money Services Businesses should have procedures for responding to foreign agents or counterparties that present unreasonable risks of money laundering or the financing of terrorism. Such procedures should provide for the implementation of corrective action on the part of the foreign agent or counterparty or for the termination of the relationship with any foreign agent or counterparty that the Money Services Business determines poses an unacceptable risk of money laundering or terrorist financing, or that has demonstrated systemic, willful, or repeated lapses in compliance with the Money Services Business' own anti-money laundering procedures or requirements.

While Money Services Businesses may already have implemented some or all of the procedures described in this Interpretive Guidance as a part of their anti-money laundering programs, we wish to provide a reasonable period of time for all affected Money Services Businesses to assess their operations, review their existing policies and programs for compliance with this Advisory, and implement any additional necessary changes. We will expect full compliance with this Interpretive Release within 180 days.

Finally, we are mindful of the potential impact that this Interpretive Release may have on continuing efforts to bring informal value transfer systems into compliance with the existing regulatory framework of the Bank Secrecy Act. Experience has demonstrated the challenges in securing compliance by, for instance, hawalas and other informal value transfer systems. Further specification of Bank Secrecy Act compliance obligations carries with it the risk of driving these businesses underground, thereby undermining our ultimate regulatory goals. On balance, however, we believe that outlining the requirements for dealing with foreign agents and counterparties, including informal networks, is appropriate in light of the risks of money laundering and the financing of terrorism.

RELEASE NO. 2004–02

This FinCEN interpretive guidance clarifies that reports filed with the Department of the Treasury's Office of Foreign Assets Control (''OFAC'') of blocked transactions with Specially Designated Global Terrorists, Specially Designated Terrorists, Foreign Terrorist Organizations, Specially Designated Narcotics Trafficker Kingpins, and Specially Designated Narcotics Traffickers will be deemed by FinCEN to fulfill the requirement to file suspicious activity reports on such transactions for purposes of FinCEN's suspicious activity reporting rules. However, the filing of a blocking report with OFAC will not be deemed to satisfy a financial institution's obligation to file a suspicious activity report if the transactions would be reportable under FinCEN's suspicious activity reporting rules even if there were no OFAC match. Moreover, to the extent that the financial institution is in possession of information not included on the blocking report filed with OFAC, a separate suspicious activity report should be filed with FinCEN including that information.

Background

The Bank Secrecy Act authorizes the Secretary of the Treasury to require financial institutions to report ''any suspicious transaction relevant to a possible violation of law or regulation.''[1] Under this authority, FinCEN has issued regulations requiring banks, securities broker-dealers, introducing brokers, casinos, futures commission merchants, and money services businesses, to report suspicious activity that meets a particular dollar threshold.[2] Each rule includes

[1] *See* 31 U.S.C. 5318(g)(1).

[2] See 31 CFR 103.17–21. The threshold for most financial institutions is $5,000; transactions conducted at points of sale for

Continued

filing procedures requiring that a suspicious transaction shall be reported by completing a suspicious activity report and filing it with FinCEN in a central location to be determined by FinCEN. Generally, the rules provide a financial institution with thirty days from the date of the initial detection of suspicious activity to file a report, with an additional thirty days if the financial institution is unable to identify a suspect. Reports are filed on forms developed for each industry subject to the reporting requirement.[3]

OFAC administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. OFAC's Reporting, Procedures and Penalties Regulations at 31 CFR part 501 require U.S. financial institutions to block and file reports on accounts, payments, or transfers in which an OFAC-designated country, entity, or individual has any interest.[4] These reports must be filed with OFAC within ten business days of the blocking of the property.[5]

Prior Guidance

Transactions involving an individual or entity designated on OFAC's list of Specially Designated Nationals and Blocked Persons as a global terrorist, terrorist, terrorist organization, narcotics trafficker, or narcotics kingpin[6] may be in furtherance of a criminal act, and therefore relevant to a possible violation of law. Thus, blocking reports related to such persons also describe potentially suspicious activity. In the November 2003 edition of its ''SAR Activity Review,''[7] FinCEN instructed financial institutions to file suspicious activity reports on verified matches of persons designated by OFAC. While this guidance ensured that the relevant information would be available to law enforcement, it also resulted in financial institutions being required to make two separate filings with the Department of the Treasury—one with OFAC pursuant to its Reporting, Procedures and Penalties Regulations, and one with FinCEN pursuant to its suspicious activity reporting rules.

Revised Guidance

FinCEN is hereby revising its prior guidance to eliminate the need for duplicative reporting in cases where a financial institution identifies a verified match with individuals or entities designated by OFAC. As of the date of publication of this interpretation, FinCEN will deem its rules requiring the filing of suspicious activity reports to be satisfied by the filing of a blocking report with OFAC in accordance with OFAC's Reporting, Penalties and Procedures Regulations. OFAC will then provide the information to FinCEN for inclusion in the suspicious activity reporting database where it will be made available to law enforcement. This construction of the suspicious activity reporting rules will serve the public interest by enabling FinCEN to obtain and provide potentially important information about terrorists and major drug traffickers to law enforcement on an expedited basis without imposing duplicative reporting burdens on the regulated industry.

Accordingly, a financial institution that files a blocking report with OFAC due to the involvement in a transaction or account of a person designated as a Specially Designated Global Terrorist, a Specially Designated Terrorist, a Foreign Terrorist Organization, a Specially Designated Narcotics Trafficker Kingpin, or a Specially Designated Narcotics Trafficker, shall be deemed to have simultaneously filed a suspicious activity report on the fact of the match with FinCEN, in satisfaction of the requirements of the applicable suspicious activity reporting rule. This interpretation does not affect a financial institution's obligation to identify and report suspicious activity beyond the fact of the OFAC match. To the extent that the financial institution is in possession of information not included on the blocking report filed with OFAC, a separate suspicious activity report should be filed with FinCEN including that information. This interpretation also does not affect a financial institution's obligation to file a suspicious activity report even if it has filed a blocking report with OFAC, to the extent that the facts and circumstances surrounding the OFAC match are independently suspicious—and are otherwise required to be reported under existing FinCEN regulations. In those cases, the OFAC blocking report would not satisfy a financial institution's suspicious activity report filing obligation.

Further, nothing in this interpretation is intended to preclude a financial institution

---

money services businesses have a reporting threshold of $2,000. See 31 CFR 103.20.

[3] See TD F 90–22.47 (depository institutions); TD F 22.56 (money services businesses); FinCEN Form 101 (securities and futures industries); FinCEN Form 102 (casinos and card clubs).

[4] 31 CFR 501.603.

[5] 31 CFR 501.603(b)(1)(i).

[6] The specific designations are as follows: Specially designated terrorist; foreign terrorist organization; specially designated global terrorist; specially designated narcotics trafficker; specially designated narcotics trafficker kingpin. *See* 31 CFR parts 595, 597, 598 and the Foreign Narcotics Kingpin Act, 21 U.S.C. 1901–08, 8 U.S.C. 1182. These categories of designations are subject solely to blocking requirements.

[7] Issue 6 (Nov. 2003).

from filing a suspicious activity report to disclose additional information concerning the OFAC match,[8] nor does it preclude a financial institution from filing a suspicious activity report if the financial institution has reason to believe that terrorism or drug trafficking is taking place, even though there is no OFAC match. Finally, this interpretation does not apply to blocking reports filed to report transactions and accounts involving persons owned by, or who are nationals of, countries subject to OFAC-administered sanctions programs. Such transactions should be reported on suspicious activity reports under the suspicious activity reporting rules if, and only, if, the activity itself appears to be suspicious under the criteria established by the suspicious activity reporting rules.

[69 FR 74439, Dec. 14, 2004, as amended at 69 FR 76847, Dec. 23, 2004]

PART 123 [RESERVED]

PART 128—REPORTING OF INTERNATIONAL CAPITAL AND FOREIGN-CURRENCY TRANSACTIONS AND POSITIONS

Subpart A—General Information

Subpart B—Reports on International Capital Transactions and Positions

Subpart C—Reports on Foreign Currency Positions

AUTHORITY: 22 U.S.C. 286f and 3101 *et seq.*; 31 U.S.C. 5315 and 5321.

[8] Such a report would be a voluntary report under the statute and regulations. *See* 31 U.S.C. 5318(g)(3) (extending safe harbor protection from civil liability to voluntary filings).

SOURCE: 58 FR 58495, Nov. 2, 1993, unless otherwise noted.

Subpart A—General Information

§ 128.1 General reporting requirements.

(a) *International capital transactions and positions.* (1) In order to implement the International Investment and Trade in Services Survey Act, as amended (22 U.S.C. 3101 *et seq.*); and E.O. 11961, and to obtain information requested by the International Monetary Fund under the articles of agreement of the Fund pursuant to section 8(a) of the Bretton Woods Agreements Act (22 U.S.C. 286f) and E.O. 10033, persons subject to the jurisdiction of the United States are required to report information pertaining to—

(i) United States claims on, and liabilities to, foreigners;

(ii) Transactions in securities and other financial assets with foreigners; and

(iii) The monetary reserves of the United States.

(2) Data pertaining to direct investment transactions are not required to be reported under this Part.

(3) Reports shall be made in such manner and at such intervals as specified by the Secretary of the Treasury. See subpart B of this part for additional requirements concerning these reports.

(b) *Foreign currency positions.* (1) In order to provide data on the nature and source of flows of mobile capital, including transactions by large United States business enterprises (as determined by the Secretary) and their foreign affiliates as required by 31 U.S.C. 5315, persons subject to the jurisdiction of the United States are required to report information pertaining to—

(i) Transactions in foreign exchange;

(ii) Transfers of credit that are, in whole or part, denominated in a foreign currency; and

(iii) The creation or acquisition of claims that reference transactions, holdings, or evaluations of foreign exchange.

(2) Reports shall be made in such manner and at such intervals as specified by the Secretary. See subpart C of