As Appeared in
Journal of Financial Crime
Vol. 10, No. 4, April 2003

Compliance Issues in the Wake of the USA PATRIOT Act

Harvey M. Silets and Carol R. Van Cleef

Financial services companies and other businesses are beginning to confront the realities of a new regulatory regime that will challenge conventional methods of conducting business, alter traditional customer expectations about their financial transactions, require investment in new technology and involve substantially greater compliance costs. This new regime was created in large part by the efforts of US policy makers to develop and enhance tools for fighting terrorism and more traditional forms of money laundering. The first step was taken on 23rd September, 2001, when President Bush signed Executive Order 13224 to freeze the assets of, and prohibit transactions with, terrorists. Efforts intensified 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') in October 2001.

Since October 2001, various US governmental entities have been working tirelessly to implement the numerous provisions of the USA PATRIOT Act that impose new recordkeeping and reporting requirements on a wide range of companies. These regulatory initiatives have potential ramifications not only for domestic (ie US-based) transactions involving US persons, but also international transactions, involving anyone living or doing business in the USA or through US companies, their foreign branches or subsidiaries.

Federally regulated depository institutions must enhance existing anti-money laundering compliance programmes, while other types of financial services and certain non-financial services companies now face new legal requirements to develop such compliance programmes. In view of substantial civil and criminal monetary and other penalties for anti-money laundering violations, other non-financial services companies also should consider adopting policies and procedures for identifying their customers, business partners and vendors, handling cash transactions and ensuring against the use of company resources in money laundering or terrorist activities by wayward employees.

This paper reviews the scope of money laundering crimes, the new requirements for anti-money laundering compliance programmes, and the Office of Foreign Assets Control requirements. It also discusses certain steps that should be considered for ensuring appropriate compliance.

MONEY LAUNDERING CRIMES

US anti-money laundering laws prohibit any person, individual, corporation or other entity from knowingly conducting or attempting to conduct a financial transaction that involves funds that are the proceeds of over 100 types of illegal activities. Terrorism and a number of other new predicate offences were added by the USA PATRIOT Act to the list of money laundering violations, which can result in substantial monetary fines, criminal penalties and asset forfeitures.[1] The provision of any type of monetary instrument to support terrorism is also a criminal offence.[2] The USA PATRIOT Act significantly broadened the authority of law enforcement officials to pursue asset forfeitures for money laundering violations.

Journal of Financial Crime
Vol. 10, No. 4, April 2003, pp. 392-399
© Henry Stewart Publications, ISSN 1359-0790
www.henrystewart.com/journals/finance.htm

ANTI-MONEY LAUNDERING COMPLIANCE PROGRAMMES

The USA PATRIOT Act amended a number of provisions in the federal Bank Secrecy Act (BSA), a recordkeeping and reporting statute, to impose new and/or enhanced requirements on all 'financial institutions' subject to the BSA. One of the most significant provisions required all such financial institutions to implement anti-money laundering (AML) compliance programmes by 24th April, 2002, unless specifically exempted by the US Treasury Department. Certain financial institutions were granted 'temporary exemptions' until late October 2002.

Such AML compliance programmes at a minimum must include internal AML policies, procedures and controls, a designated AML compliance officer, an ongoing employee-training programme and an independent audit function. Policies and procedures designed to implement other requirements of the USA PATRIOT Act — including enhanced due diligence procedures with respect to certain types of customer relationships, new customer identification programmes, and suspicious activity reporting — must be incorporated into AML compliance programmes. The specific requirements are discussed in greater detail in KMZR's 'USA PATRIOT Act: Statutory Analysis and Regulatory Implementation', which is available on the KMZR website.

Wide range of companies covered

For purposes of the BSA, the term 'financial institution' is broadly defined to include not only federally insured depository institutions, but also a wide range of financial services and other companies. This list includes many, but not all, of the organisations subject to the privacy provisions of the federal Gramm-Leach-Bliley Act, as well as additional organisations.

The following types of organisations are expressly defined by the BSA to be financial institutions and, therefore, subject to the USA PATRIOT Act's section 352 requirements for AML compliance programme (unless specifically exempted by the Treasury Department):[3]

- Federally insured bank, thrift or credit union
- Private banker
- Uninsured commercial bank, trust company or thrift
- US branch or agency of a foreign bank
- Registered securities broker or dealer
- Broker or dealer in securities or commodities
- Investment banker
- Investment company
- Futures commission merchant
- Commodity trading adviser
- Commodity pool operator
- Casino or gaming establishment
- Operator of a credit card system
- Business engaged in automobile, airplane and boat sales
- Insurance company
- Loan or finance company
- Persons involved in real estate closings and settlements
- Issuer, redeemer, or cashier of travellers' cheques, money orders or similar instruments
- Currency exchange
- Licensed sender of money
- Any other person engaging as a business in the transmission of funds
- Pawnbroker
- Dealer in precious metals, stones or jewels
- Travel agency
- US Postal Service
- Telegraph company
- Federal, state or local government agency carrying out a duty or power of a business or a financial institution

The Treasury Secretary also has broad discretion to impose the section 352 AML compliance programme requirement on any other business engaging in (a) similar or related activities, or (b) cash transactions with a high degree of usefulness in criminal, tax or regulatory matters.

Pre-PATRIOT Act compliance programmes

Prior to the enactment of the USA PATRIOT Act, the BSA reporting and recordkeeping requirements were imposed only on a limited number of such 'financial institutions'. Federally insured depository institutions were the most heavily regulated. Registered broker-dealers, money services businesses (including cheque sellers) (MSBs) and casinos also were subject to regulation, albeit to a somewhat lesser degree.[4]

The Treasury Department, which is responsible for implementing the BSA, had the option before the USA PATRIOT Act of requiring all entities subject to the BSA to develop AML compliance programmes. The federal bank regulators required all federally insured depository institutions and bank holding companies to adopt 'Bank Secrecy Act compliance programmes' which are virtually identical to the s. 352 requirement. The Financial Crimes Enforcement Network (FinCEN), however, did not require any type of financial institutions subject to the BSA — other than casinos — to adopt such a programme.[5]

Required AML compliance programmes

Pursuant to Treasury regulations, banks, thrifts, credit unions, registered broker-dealers, casinos, and futures commission merchants and introducing brokers were required to have AML compliance programmes by 24th April, 2002. MSBs, mutual funds and operators of credit card systems were required to implement programmes by 24th July, 2002. On 26th September, 2002, the Treasury Department proposed for public comment regulations requiring life insurance companies and unregistered investment companies to implement AML compliance programmes. FinCEN is expected over the next several months to promulgate additional regulations for other groups of financial institutions as it resolves the issue of which of these entities are financial institutions for purposes of the BSA, and which of such financial institutions should be subject to the s. 352 requirement.

Exempted entities

Since the USA PATRIOT Act made AML compliance programmes mandatory for any entity not expressly excluded by regulation, the Treasury Department must affirmatively act to exempt organisations. As noted above, a temporary exemption was granted to all entities considered financial institutions under the BSA but not already subject to Treasury regulations implementing s. 352. This exemption, however, lasts only until Treasury can resolve which of the many businesses potentially subject to the BSA should be deemed 'financial institutions', and in turn required to have AML compliance programmes.

The Treasury Department is currently wrestling with many of these questions. For example, it must determine which of the various types of companies that technically qualify as 'loan or finance companies' — including leasing companies that make leases which are the functional equivalent of loans — should be financial institutions and of these, which should be subject to the s. 352 requirement. It also has been considering whether payroll processors and ACH processors are MSBs under the regulation and thus required to have programmes.

With respect to the definition of 'insurance companies', the Treasury Department has proposed to include only life insurance companies and other companies whose products include annuities or insurance products with investment features similar to those of a life insurance policy or annuity or which can be used to store value and transfer that value to another person. As proposed, insurance agents as well as brokers would not generally be subject to this rule, although life insurance companies would be responsible for determining the extent to which their insurance agents (either captive or independent) should be subject to AML compliance policies and procedures. Also the proposed rules would not subject either health, property or casualty companies to s. 352's requirement. The Treasury Department has asked for comment on whether those insurance companies excluded from the definition, as well as agents and brokers, should be covered.

The Treasury Department has also proposed a sweeping definition of unregistered investment companies that would include, with only limited exceptions, hedge funds, commodity pools and companies that invest primarily in real estate and or interests therein. As proposed, this rule would cover any such company that has assets of $1m or more (measured quarterly), permits ownership interests to be redeemed within two years of purchase and either (a) is organised under US or state law, (b) is organised, operated or sponsored by a US person or (c) sells ownership interests to a US person.

The comment period for both proposals ends on 25th November, 2002. Implementation of AML programmes for unregistered investment companies will be required within 90 days after the regulations are published in final form.

The Treasury Department has already spent several months working through these issues. It is expected to take several more months to complete the task. In the interim, some of the 'temporary exemptions', which expire on 24th October, 2002, may need to be extended.

Programme components

The regulations published to date reiterate the statutory requirements but provide little detail on the actual components of a required AML compliance

programme. Generally, the regulations stress that organisations have flexibility to develop policies, procedures and controls that are *risk-based* and reflect the anti-money laundering risks that a particular company or industry encounters. This flexibility provides entities with substantial discretion to craft an AML compliance programme that is reasonably designed to prevent the entity from being used to facilitate money laundering or financing of terrorist activities. The programme should address the unique aspects of their businesses and products, the size and location of the company, the nature and location of the customers and other considerations.

Typical elements of AML compliance programmes required by the Treasury regulations promulgated to date include the following (not all requirements may apply initially and may require additional rulemaking before becoming effective):

— Policies, procedures and controls with provisions for:
- verifying customer identification (regulations proposed)
- filing required reports (currency transaction reports (CTRs), suspicious activity reports (SARs) and others)
- creating and maintaining required reports (including reports on wire transfers) responding to law enforcement requests
- integrating due diligence and enhanced due diligence programmes for correspondent and private banking accounts (required under other regulations)

— An AML compliance officer with responsibility for assuring day-to-day compliance with respect to:
- properly filing reports and creating and retaining required records
- updating the programme to reflect current regulatory requirements
- providing appropriate employee education and training

— Education and training for appropriate personnel concerning their responsibilities and including training in the detection of suspicious transactions

— Independent audit conducted
- with a scope and frequency commensurate with the money laundering risks posed by the business
- by either an outside party or by an officer or employee of the entity other than the compliance officer

Most industry-specific regulations require the programmes to be in writing and approved by either the board of directors or senior management. The programmes also must be made available to the Treasury Department or its designee upon request. Casinos and MSBs have been required to integrate their programmes with existing automated data processing systems.

Enforcement and violations

As noted above, FinCEN, pursuant to delegated authority from the Treasury Department, is responsible for determining violations under the BSA and determining what, if any, sanctions are appropriate. Entities such as banks and registered broker-dealers that have a federal functional regulator will be regularly examined by that regulator for BSA compliance, and referrals for enforcement action will be made to FinCEN when appropriate.[6] The IRS and state regulators will review compliance by MSBs, and the state insurance regulators also will likely review insurance company compliance. Authority to investigate criminal violations of the BSA is delegated to the IRS. It is likely that the IRS will similarly be authorised to examine and investigate other entities that do not have a federal functional regulator as they become subject to various provisions, including s. 352 of the BSA.

Violations of the BSA and implementing regulations can result in civil money penalties and criminal fines of up to $lm per day of continuing violation and possible imprisonment. The Department of Justice may prosecute criminal violations upon referral.

Two recent orders by FinCEN are indicative of the determined efforts to prosecute violations of the BSA. In one case, FinCEN fined a banking organisation $700,000 for failing to monitor and supervise the compliance activities of a service provider (an armoured-car carrier) in connection with services provided to the bank.[7] The service provider failed to complete the required CTRs on the bank's behalf and the bank failed to monitor the activities of the service provider to ensure the CTRs were being filed. Once the bank became aware of the situation and started filing the CTRs itself, it failed to verify that it had received an accurate customer list from the service provider. The bank also failed to monitor adequately the activities of a second service provider that had assumed part of the bank's compliance responsibilities.

The second order involved a small banking organisation that had total assets of $55m, earnings of $250,000 in the most recent fiscal year and $40,000 in income for the most recent six-month period.[8] FinCEN fined this organisation $100,000 for wilful violations of the BSA. FinCEN said that even after the bank was on notice by its regulator that it had material deficiencies in its SAR compliance programme, it failed to establish appropriate corrective procedures that would 'reasonably assure' proper reporting. FinCEN said, failing to establish procedures to adequately identify, document and report suspicious transactions, particularly after being put on notice repeatedly of serious compliance deficiencies, is following a course of conduct that demonstrates reckless disregard for compliance. The bank wilfully violated the SAR reporting requirements because it did not have any procedures to identify or analyse 'even the most conspicuous suspicious activities' or properly document and monitor records for those that it did report, and failed to comply with the SAR requirements in numerous instances.

OFFICE OF FOREIGN ASSETS CONTROL

The Office of Foreign Assets Control (OFAC) is the office within the US Treasury Department responsible for administering a number of programmes that implement more than ten different statutory schemes affecting transactions with various foreign countries, governments, entities and individuals. Each one of these statutes has specific compliance requirements and, in varying degrees, they prohibit business dealings with and require the blocking of transactions involving such foreign countries, governments, entities and individuals.

This regulatory framework has been in existence since World War II. However, it attracted little attention outside the import/export sectors until the issuance of Executive Order 13224 (the 'Executive Order') by President Bush on 23rd September, 2001.

Executive Order

The Executive Order requires the blocking of 'all property and interests in property' of (a) certain named terrorists; (b) other foreign persons deemed to have committed or to pose the threat of committing acts of terrorism; (c) persons owned or controlled by or acting for or on behalf either of the above; (d) any persons (including charities) assisting in, sponsoring or providing financial, material or technological support for, or financial services to or in support of, terrorism or a person subject to the Executive Order; and (e) anyone otherwise associated with persons covered by the Executive Order. The Executive Order also broadly prohibits any transactions or dealings (a) by US persons or (b) within the USA in property or interests in property blocked by the order. The Executive Order generally applies to all US citizens, resident aliens, US corporations (and foreign branches) and any other individual or entity in the USA.[9] The Executive Order effectively imposes a very significant duty on all parties to know not only all of the other parties in a transaction, but also their own employees to ensure the Executive Order is not violated. OFAC maintains a list of persons and entities whose assets are to be blocked. This list is called the List of Specifically Designated Nationals and Blocked Persons.

UN List

The individuals and entities appearing on this list are also submitted to the United Nations for inclusion on a similar list maintained by the UN Sanctions Committee established pursuant to UN Security Council Resolution 1267. Members of the United Nations are required to similarly block assets of, and prohibit transactions with, individuals and entities on this list.

Enforcement and penalties

OFAC administers a draconian system of civil money penalties and criminal fines and makes referrals to the US Department of justice for criminal prosecution. OFAC generally enforces the statute on a strict liability basis — if a violation occurs, a penalty will be assessed. OFAC may treat an existing compliance programme or the establishment of a new compliance programme as a mitigating factor in the penalty stage of an enforcement action to lessen the severity of the penalty.

OFAC will also consider as a mitigating factor the use of interdiction software that can automate the review of names on the rapidly growing list prepared by OFAC of specially designated nationals and entities with whom transactions are prohibited. OFAC, however, cautions against developing a compliance programme that relies solely on an automated review of these lists because not all parties subject to OFAC sanctions will appear on the list. A 'positive hit' may only be the start of the inquiry necessary to identify whether a party is subject to sanctions, and further inquiry may be necessary when a similar but not identical name is identified.

Federal functional regulators and some state regulators review for compliance with OFAC rules and regulations during examination and may, as necessary, refer violations of such rules to OFAC. Proposed Treasury rules would require review of the OFAC list to be incorporated into s. 352 compliance pro-grammes, increasing liability for failure to comply with OFAC rules.

Limited safe harbour

OFAC has been extraordinarily reluctant to create any type of safe harbour from the regulations it enforces. It has created a limited safe harbour with respect to certain domestic automated clearing house (ACH) transactions, which generally are low-dollar value, high-volume wire transfers. This safe harbour permits an originating depository financial institution (ODFI) in such wire transfers to shift responsibility for OFAC compliance in domestic transactions to receiving depository financial institutions (RDFI) if the ODFI requires a commitment from the ACH originator to comply with OFAC rules and includes language to that effect in its ACH agreements with ACH originators.

The NACHA Operating Rules have codified this interpretation, although it applies to agreements entered into only after 19th September, 1997.[10] The NACHA rule requires the ODFI to verify that the originator is not a blocked party and to undertake a good faith effort to determine, through the normal course of business, that the originator is not engaged in transmitting funds to, from, or on behalf of a party subject to such sanctions. Also, if the ODFI encounters a transaction initiated by an originator that violates the OFAC sanctions, the ODFI must comply with the OFAC policies and block the transaction or freeze the assets.

OFAC reserves the right to look at individual ACH transactions. International ACH transactions are not subject to this 'understanding'.

COMPLIANCE CONSIDERATIONS

The regulations requiring AML compliance programmes under s. 352, the Executive Order, and other OFAC rules impose new compliance burdens on many entities that previously have been either unregulated or lightly regulated. The burdens are far-reaching and require entities to know not only their clients and their clients' employees, but their own employees as well.

Existing programmes

Entities that have AML and OFAC compliance policies and procedures already in place should carefully review them to ensure that they reflect the new and revised regulatory changes being implemented pursuant to the USA PATRIOT Act. In addition, entities should ensure that their procedures can be properly implemented (especially if significant portions of these operations are outsourced). Federal functional regulators increasingly are examining not just for the existence of AML compliance programmes, but also for how well they work. Conducting such a review under the attorney-client privilege will provide an organisation with certain legal protections while it addresses any shortcomings that may be revealed.

Determining s. 352's applicability

Companies with US operations or doing business with US companies or their affiliates should review their operations to determine the extent to which all or part of such operations may fall within the BSA's broad definition of the term 'financial institution' or are otherwise subject to specified BSA requirements (eg currency transaction reporting requirements). A foreign corporation that does not do business in the USA but does business with a US company may not be directly subjected to, but may find itself impacted by, certain Treasury rules if it falls within the BSA definition of the term 'financial institution'. OFAC rules apply to all organisations without regard to the applicability of s. 352.

Temporarily exempted organisations

Entities granted a temporary exemption from s. 352's AML compliance programme requirements are still subject to the anti-money laundering statutes and the BSA, which require the reporting of one or more related transactions involving the receipt in cash or cash equivalents in excess of $10,000 and the existence of foreign banking, securities and other financial accounts. Other requirements also may apply.

Flexibility and allocating compliance

The flexibility of the Treasury Department regulations specifying s. 352 AML compliance programme requirements allows organisations to tailor their programmes to the money laundering and terrorism financing risks potentially facing their operations. With appropriate oversight, parts of the compliance burden (but not the liability) may be allocated to other entities. For example, in the case of MSBs, the MSB and its

agents may allocate responsibility for the development of policies, procedures and internal controls. Each, however, remains 'solely responsible' for implementation of the regulatory requirements, and neither is relieved of its obligation to establish and maintain an effective AML compliance programme. Oversight will help ensure that a third party's activities comply with the terms of the allocation agreement and help avoid potential substantial penalties for violations.

Deadline for temporarily exempted organisations

The Treasury Department announced on 11th October that it would 'shortly' provide guidance with respect to regulations that must be issued before the end of October. Presumably, the Treasury Department will extend the temporary exemption for those companies for which regulations have not yet been finalised. Otherwise, the companies will be required to be in compliance with s. 352 and have implemented AML compliance programmes by 24th October, 2002.

Suspicious activity reporting

The Treasury Department has reminded all entities subject to the Bank Secrecy Act of the 'importance of reporting suspected terrorist activities or otherwise suspicious transactions' to the appropriate law enforcement authorities. It encourages organisations not yet required to file a suspicious activity report to make such a filing voluntarily. It also has proposed SAR, requirements for life insurance companies and currency dealers and exchangers.

State laws

State anti-money laundering requirements may apply.

Early adoption

Companies should consider developing AML compliance programmes in whole or in part before industry-specific regulations become final. For example, insurance companies that are registered broker-dealers for the sale of variable rate annuity products are currently required to have an AML compliance programme in place. Also, contractual partners and vendors are increasingly seeking representations and warranties as to the existence and effectiveness of internal AML compliance programmes or compliance with applicable laws. In addition, parties to contracts involving financial, real estate and other types of transactions are being asked to make representations with respect to their compliance with OFAC, and sometimes anti-money laundering statutory and regulatory requirements. Depending on the nature of the party agreeing to make such a representation, substantial internal due diligence and the adoption of certain procedures may be necessary to lessen liability under such clauses.

OFAC compliance

The OFAC requirements are ubiquitous. They impose a burden with respect to all transactions, and only narrowly circumscribed relief is provided for a limited group of small dollar wire transactions as discussed above. OFAC compliance programmes are not required but can serve to mitigate penalties if a violation occurs.

AML and OFAC compliance programmes for other entities

Certain provisions of the BSA apply to all entities regardless of whether they are deemed financial institutions — reporting receipt of cash or cash equivalents over $10,000 to FinCEN and periodic filings and record keeping with respect to foreign bank, securities or other financial accounts. In light of these requirements and the criminal liability of the money laundering statutes that may be imposed for violations, all entities should consider adopting a basic set of anti-money laundering policies and procedures to ensure compliance with any applicable requirements. Such policies and procedures, however, are not required to comply with the requirements of s. 352. An OFAC policy should similarly be considered.

Privacy

Development of an effective AML compliance programme is likely to raise certain privacy issues, especially for companies with foreign (ie non-US) operations.

CONCLUSION

The consequences of non-compliance with AML and OFAC statutes and regulations can be severe, if not devastating, for an organisation. Non-compliance may result in substantial civil and criminal penalties and, in the case of insured depository institutions, possible loss of charter or federal deposit insurance coverage. Because implementation of the USA PATRIOT Act will be an ongoing process for the foreseeable future, adequate compliance can be ensured only with regular review and revision of existing policies and procedures in light of new and revised regulations.

REFERENCES

(1) See 18 USC §§1956, 1957. A financial transaction for purposes of this provision includes a transaction affecting interstate or foreign commerce involving the movement of funds by wire or other means or a transaction involving the use of a financial institution which is engaged in, or the activities of which affect, interstate or foreign commerce in any way.

(2) See 18 USC §2339a.

(3) See 31 USC §5312(a)(2).

(4) As of 31st December, 2001, MSBs were required to register with the Treasury Department. Beginning at 1st January, 2002, they were required to file suspicious activity reports (SARs). Rules requiring the filing of SARs by broker-dealers become applicable at the end of 2002. The Treasury Department has published final rules requiring casinos and card clubs to file SARs. Proposed SAR requirements for life insurance companies and currency dealers and exchangers were published by the Treasury Department on 17th October, 2002.

(5) See 31 CFR §103.64.

(6) See 31 CFR §103.56.

(7) *In the Matter of Sovereign Bank*, 8th April, 2002; http:// www.treas.gov/fincen/sovereignbank.pdf

(8) *In the Matter of Great Eastern Bank of Florida*, 4th September, 2002; http://www.treas.gov/fincen/geassessfinal.pdf

(9) Some OFAC programmes also cover foreign subsidiaries of US corporations.

(10) See NACHA Operating Rule 2.1.1 and accompanying NACHA 2002 Operating Guidelines.

Harvey M. Silets *is a partner in the Chicago office of the law firm Katten Muchin Zavis Rosenman.*

Carol R. Van Cleef *is a partner in the Washington, DC office of Katten Muchin Zavis Rosenman. For questions or further information please contact Carol R. Van Cleef at 001 202 625 3730 or carol.vancleef@kmzr.com.*