31

THE U.S. PATRIOT ACT AND RELATED DOMESTIC AND INTERNATIONAL ANTI-MONEY LAUNDERING REGULATIONS, WITH A SPECIAL FOCUS ON SWITZERLAND: LEGAL AND BUSINESS IMPLICATIONS

Raymond L. Moss
Sims Moss Kline & Davis LLP
Lionel Aeschlimann
Schellenberg Wittmer
Gerald B. Kline
Gilbert H. Davis
Sims Moss Kline & Davis LLP

Table of Contents

I. Overview

In a swift response to the terrorists attacks on September 11, 2001, the U.S. Congress passed the USA Patriot Act (the "Act").[1] The Act gives, among other things, U.S. federal officials greater authority to track and intercept communications, both for law enforcement and foreign intelligence gathering purposes. It also vests in the U.S. Secretary of the Treasury regulatory powers to combat corruption of U.S. financial institutions for foreign money laundering purposes. It also seeks to close U.S. borders to foreign terrorists and to detain and remove terrorists from U.S. borders. It creates new crimes, new penalties, and new procedural mechanisms for use against domestic and international terrorism.

The provisions of the Act which affect banking organizations and other "financial institutions" are generally set forth as amendments to the Bank Secrecy Act. The Act is far reaching in scope, covering a broad range of financial institutions and activities. The Act and related regulations define the term "financial institution" quite broadly and includes within its definition banks insured under the Federal Deposit Insurance Act; commercial banks or trust companies; agencies or branches of foreign banks in the United States; thrift institutions; brokers or dealers and mutual funds registered with the U.S. Securities and Exchange Commission ("SEC"); mutual funds; and a long list of other entities including, but not limited to, businesses engaged in the sale of automobiles, airplanes, and boats; insurance companies; travel agencies; and pawn brokers.

This chapter will generally focus on the Act's implications on financial institutions, including broker-dealers, mutual funds, investment advisers, and hedge funds both in the U.S. and abroad. It will then provide an outline of selected legal initiatives that have been taken over the last years by international organizations and private business associations to fight money laundering and terrorism financing. Finally, this chapter will describe the main characteristics of the legal and regulatory framework that has been designed and implemented in an important international financial center, namely Switzerland, to combat money laundering and international criminality, including terrorism financing.

II. Current Law, Rules, and Regulations In the U.S.

A. Money Laundering Under the Bank Secrecy Act and the Act

Money laundering is the flow of cash or other valuables derived from, or intended to facilitate the commission of a criminal offense. It is the movement of the fruits and instruments of crime.[2]

---

[1] P.L. 107-56, 115 Stat. 272 (2001), *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act)*.

[2] *The U.S. Patriot Act, A Legal Analysis*, Charles Doyle, Congressional Research Service, Library of Congress, CRS Report for Congress, Order Code RL31377.

Prior to the passage of the Act, the U.S. Treasury Department already had significant authority with regard to requiring reporting and record keeping standards on financial institutions generally and specifically with respect to money laundering matters.[3] For example, under the Currency and Financial Transaction Reporting Act, a component of the Bank Secrecy Act, anyone who transports more than $10,000 into or out of the United States must report that fact to the Treasury Department.[4] Banks, credit unions, and certain other financial institutions were also required to identify information relating to cash transactions in excess of $10,000 to the U.S. Treasury Department.[5] Banks must file suspicious activity reports ("SAR's") with the U.S. Treasury Department's Financial Crimes Enforcement Network ("FinCEN") for any transaction involving more than $5,000 which they suspect may be derived from illegal activity.[6] Money transmission business and those that deal in travelers checks or money orders are under similar obligations for suspicious activities involving amounts in excess of $2,000.[7]

The Act, among other things, greatly enhances the authority of the U.S. Secretary of the Treasury regarding these reporting requirements. Pursuant to this authority, the U.S. Secretary of the Treasury has the power to promulgate regulations governing securities brokers and dealers as well as commodity merchants, advisers, pool operators, and other financial institutions.[8] For example, under the Act, businesses which were only required to report cash transactions involving more than $10,000 to the IRS are now required to file SAR's as well.[9] At the same time, under the Act, financial institutions and their directors, officers, employees, and agents are protected from liability for such reporting of suspicious banking activities. Similar provisions also apply to broker-dealers registered with the U.S. Securities and Exchange Commission. In addition, the Fair Credit Reporting Act has been amended to allow consumer reporting agencies to provide consumer reports to governmental agencies for counter-terrorism purposes.

FinCEN, a component within the Treasury Department, historically responsible for the reporting of anti-money laundering and record keeping, was created

---

[3] *See, e.g.,* 12 U.S.C. 1829b, "retention or records by insured depository institutions," 1951 and 1959 (record keeping by financial institutions; 31 U.S.C. 5311).

[4] 31 U.S.C. 5316.

[5] 31 U.S.C. 5313, 31 C.F.R. §103.22.

[6] 31 U.S.C. 5318(g), 31 C.F.R. §103.18.

[7] 31 U.S.C. 5318(g), 31 C.F.R. §103.18.

[8] 31 U.S.C. 5313; 31 U.S.C. 5312(c)(1).

[9] §365, 31 U.S.C. 5331; §321, 31 U.S.C. 5312.

administratively in 1990 to provide other government agencies with "intelligence and an analytical network in support of the detection, investigation, and prosecution of domestic and international money laundering and other financial crimes."[10] The Act, in section 361, makes FinCEN a statutory creation as a bureau of the Department of the Treasury.[11]

In extraordinary circumstances involving international financial matters, the Act grants the Secretary of the Treasury, in consultation with certain other regulatory agencies, the power to issue regulations and orders involving additional required "special measures" and additional "due diligence" requirements to combat money laundering.[12] These powers are potentially quite broad.

B. Due Diligence Under the Act

Section 312 of the Act requires that all U.S. financial institutions have policies, procedures, and controls in place to identify circumstances where the correspondent and private banking accounts of such financial institutions with foreign individuals and entities might be used for money laundering purposes.[13] In addition, the Act requires enhanced due diligence standards for correspondent accounts held for offshore banking institutions (whose licenses prohibit them from conducting financial activities in the jurisdiction in which they are licensed) or institutions in money laundering jurisdictions designated by the Secretary of the Treasury or by international watchdog groups such as the Financial Action Task Force ("FATF").[14] The standards require at a minimum reasonable efforts to identify the ownership of foreign institutions which are not publicly held; closely monitor the accounts for money laundering activity; and to hold any foreign bank, for which the financial institution has a correspondent account, to the same standards with respect to other correspondent accounts maintained by the foreign bank.

With respect to private banking accounts of $1 million or more, U.S. financial institutions are now required to keep records of the owners of the accounts and the source of funds deposited in the accounts. They are also required to report suspicious

---

[10] 55 Fed. Reg. 18433, May 2, 1990.

[11] 31 U.S.C. 310.

[12] 31 U.S.C. 5318(a).

[13] 31 U.S.C. 5318(i).

[14] FATF is an inter-governmental body established by the G7 Summit in Paris, France, in July 1989 to examine measures to combat money laundering worldwide. It is comprised of representatives of the financial, regulatory, and law enforcement communities for over 31 jurisdictions and serves as a world leader in the development of effective anti-money laundering programs. *See also* FATF-GAFI Report on Money Laundering Typologies 2001-2002, February 1, 2002.

administratively in 1990 to provide other government agencies with "intelligence and an analytical network in support of the detection, investigation, and prosecution of domestic and international money laundering and other financial crimes."[10] The Act, in section 361, makes FinCEN a statutory creation as a bureau of the Department of the Treasury.[11]

In extraordinary circumstances involving international financial matters, the Act grants the Secretary of the Treasury, in consultation with certain other regulatory agencies, the power to issue regulations and orders involving additional required "special measures" and additional "due diligence" requirements to combat money laundering.[12] These powers are potentially quite broad.

B. Due Diligence Under the Act

Section 312 of the Act requires that all U.S. financial institutions have policies, procedures, and controls in place to identify circumstances where the correspondent and private banking accounts of such financial institutions with foreign individuals and entities might be used for money laundering purposes.[13] In addition, the Act requires enhanced due diligence standards for correspondent accounts held for offshore banking institutions (whose licenses prohibit them from conducting financial activities in the jurisdiction in which they are licensed) or institutions in money laundering jurisdictions designated by the Secretary of the Treasury or by international watchdog groups such as the Financial Action Task Force ("FATF").[14] The standards require at a minimum reasonable efforts to identify the ownership of foreign institutions which are not publicly held; closely monitor the accounts for money laundering activity; and to hold any foreign bank, for which the financial institution has a correspondent account, to the same standards with respect to other correspondent accounts maintained by the foreign bank.

With respect to private banking accounts of $1 million or more, U.S. financial institutions are now required to keep records of the owners of the accounts and the source of funds deposited in the accounts. They are also required to report suspicious

---

[10] 55 Fed. Reg. 18433, May 2, 1990.

[11] 31 U.S.C. 310.

[12] 31 U.S.C. 5318(a).

[13] 31 U.S.C. 5318(i).

[14] FATF is an inter-governmental body established by the G7 Summit in Paris, France, in July 1989 to examine measures to combat money laundering worldwide. It is comprised of representatives of the financial, regulatory, and law enforcement communities for over 31 jurisdictions and serves as a world leader in the development of effective anti-money laundering programs. *See also* FATF-GAFI Report on Money Laundering Typologies 2001-2002, February 1, 2002.

transactions and when the accounts are held for foreign officials, guard against transactions involving foreign official corruption.[15]

The Act also provides several other initiatives aimed at the activities of U.S. financial institutions and foreign individuals or institutions. For example, Section 313 of the Act prohibits U.S. financial institutions from maintaining correspondent accounts either directly or indirectly for foreign shell banks (banks with no physical place of business) which have no affiliation with any financial institutions through which their banking activities are subject to regulatory supervision.[16] Section 326 of the Act provides that the Secretary of the Treasury has the power to issue regulations for financial institutions, including new customer identification standards and record keeping, and to recommend a means to effectively verify the identification of foreign customers.[17] The term "customers," as used in this section, was intended to be defined by the functional regulators regulating the institutions of such customers as was done in the Gramm-Leach-Bliley Act of 1999. Under this approach, where an investment company sells its shares to the public through a broker-dealer, and maintains a street name or omnibus account in the broker-dealer's name, the purchasers of the mutual fund shares are deemed to be customers of the broker-dealer rather than the mutual fund. Under this interpretation, the mutual fund is not obligated to "look through" the broker-dealer to identify and verify the identities of such customers. In a similar manner, where an investment company sells its shares to a qualified retirement plan, the plan, rather than its participants, are deemed to be customers of the fund. Section 326 of the Act applies to all "financial institutions."

This term is defined broadly in the Act to encompass a variety of entities, including commercial banks, agencies, and branches of foreign banks of the United States, thrifts, credit unions, private banks, trust companies, brokers and dealers in securities, investment companies, futures commission merchants, insurance companies, travel agents, pawn brokers, dealers in precious metals, check cashers, casinos, and telegraph companies, among others.[18]

---

[15] *See* H.R. Rep. No. 107-250, at 71-2 ("[§312] amends 31 U.S.C. 5318 to require financial institutions that establish, maintain, administer or manage private banking or correspondent accounts for non-U.S. persons to establish appropriate, specific and, where necessary, enhanced due diligence policies, procedures, and controls to detect and report instances of money laundering through those accounts. The enhanced due diligence procedures include (1) ascertaining the identity of each of the owners of the foreign bank (except for banks that are publicly traded); (2) conducting enhanced scrutiny of the correspondent account to guard against money laundering and report any suspicious activity; and (3) ascertaining whether the foreign bank provides correspondent accounts to other foreign banks and, if so, the identity of those foreign banks and related due diligence information.

[16] 31 U.S.C. 5318(j); H.R. Rep. No. 107-250, at 72 (2001).

[17] 31 U.S.C. 5318(l); H.R. Rep. No. 107-250, at 62-3 (2001).

[18] *See* 31 U.S.C. 5312(a)(2), 5312(c)(1)(A). For any financial institution engaged in financial activities as described in the Bank Holding Company Act of 1956, the Secretary is required to prescribe the regulations issued under §326 jointly with the Office of the Controller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of Thrift

As part of the Act, the regulations implementing §326 must require, at a minimum, financial institutions to implement reasonable customer identification procedures for (1) verifying the identity of any person seeking to open an account, to the extent reasonable and practical; (2) maintaining records of the information used to verify the person's identity, including name, address, and other identifying information; and (3) determining whether the persons appearing on a list of known or suspected terrorists or terrorists organizations provided to the financial institution by any government agency.[19]

C. NASD Rule 3011 and Implications for Broker-Dealers

The Act requires all financial institutions, including brokers-dealers, to develop and implement anti-money laundering compliance programs on or before April 24, 2002. Both the NASD and the New York Stock Exchange have anti-money laundering rules - Rule 3011 and Rule 445, respectively.

Rule 3011 sets forth minimum standards for brokers-dealers' anti-money laundering ("AML") compliance programs. It requires firms to develop and implement a written AML compliance program. The program has to be approved in writing by a member of senior management and be reasonably designed to achieve and monitor the member's ongoing compliance with the requirements of the Bank Secrecy Act and the implementing of regulations promulgated thereunder. Consistent with the Act, NASD Rule 3011 also requires firms at a minimum to:

- ξ establish and implement policies and procedures that can be reasonably expected to detect and cause the reporting of suspicious transactions;
- ξ establish and implement policies and procedures and internal controls reasonably designed to achieve compliance with the Bank Secrecy Act in implementing regulations;
- ξ provide for independent testing for compliance to be conducted by member personnel or by a qualified outside party;
- ξ designate and identify to the NASD an individual or individuals responsible for implementing and monitoring day-to-day operations and internal controls of the program and provide prompt notification to the NASD regarding any change of such designations; and

---

Supervision, and the National Credit Union Administration, the Securities and Exchange Commission, and the Commodities Futures Trading Commission.

[19] SEC, Release No. 34-47752, File No. S7-25-02. Effective June 9, 2003, pursuant to a joint final rule of the Financial Crimes Enforcement Network (FinCEN), the U.S. Treasury, and the Securities and Exchange Commission, the joint final rule to implement §326 of the Act went into effect. SEC Release No. 34-47752, File No. 57-25-02.

- provide ongoing training for appropriate personnel.[20]

Section 356 of the Act requires that SAR's be filed with the FinCEN. The final rule requires broker-dealers to report to FinCEN any transaction that, alone or in the aggregate, involves at least $5,000 in funds or other assets, if the broker-dealer knows, suspects, or has reason to suspect that falls within one of four classes:

- the transaction involves funds derived from illegal activity or is intended or conducted to hide or disguise funds or assets derived from legal activities;

- the transaction is designed, whether through structure or other means, to evade the requirements of the Bank Secrecy Act;

- the transaction appears to serve no business or lawful purpose or is not the sort of transaction which the particular customer should be expected to be engaged for which the broker-dealer know of no reasonable explanation after examining the available facts; or

- the transaction involves the use of the broker-dealer to facilitate criminal activity.[21]

The SAR reporting requirement is not limited to individual transactions. FinCEN's rule extends to patterns of transactions. In its release adopting the final rule, FinCEN explicitly clarified that "if a broker-dealer determines that a series of transactions that would not independently trigger the suspicion of the broker-dealer, but that, taken together from a suspicious pattern of activity, the broker-dealer must file a Suspicious Transaction Report." NASD Rule 3011 defines a customer as (a) a person that opens a new account; and (b) an individual who opens a new account for an individual who lacks legal capacity or for an entity that is not a legal person. Under this definition, "customer" does not refer to persons who fill out account opening paperwork and who provide information necessary to set up an account if such persons are not the account holder as well.[22]

A broker-dealer is not required to look through a trust or similar account to its beneficiaries, but is required only to verify the identity of the named account holder. Similarly, with respect to an omnibus account established by an intermediary, a broker-

---

[20] NASD Anti-Money Laundering Frequently Asked Questions, Updated December 15, 2003, Question 2.

[21] *See* NASD Notice to Members 02-47.

[22] *See* NASD Anti-Money Laundering Frequently Asked Questions, Updated December 15, 2003, Question 16.

dealer is not required to look through the intermediary to the underlying beneficial owners, if the intermediary is identified as the account holder.[23]

The final rule does not include persons with trading authority over accounts in the definition of "customer." Accordingly, the broker-dealer does not have to verify those individuals' identities. However, the final rule recognizes that situations may arise where a broker-dealer will have to take extra steps to verify the identity of those with trading authority. In those instances, a CIP is required to address situations where the broker-dealer will take additional steps to verify the identity of a customer that is not an individual by seeking information about individuals with authority or control over the account in order to verify the customer's identity.[24]

Rule 3011 defines an "account" as a "formal relationship with a broker-dealer established to effect transactions and securities, including, but not limited to, the purchase or sale of securities, securities loan and barred activity, and the holding of securities or other assets for safekeeping or as collateral." Importantly, the final rule contains two exclusions from the definition of "account." The definition excludes (a) an account that the broker-dealer requires through any acquisition, merger, purchase of assets, or assumptions of liabilities and (b) an account opened for the purpose of participating in an employee benefit plan established under the Employment Retirement Income Security Act of 1974.[25] NASD Rule 3011 requires that a broker-dealer's CIP must identify the identifying information that will be obtained from each customer and must contain procedures for obtaining this identifying information.[26] At a minimum, the following information must be obtained from a customer prior to opening an account:

- a name;
- a date of birth for an individual;

---

[23] *See* NASD Anti-Money Laundering Frequently Asked Questions, Updated December 15, 2003, Question 17.

[24] *See* NASD Anti-Money Laundering Frequently Asked Questions, Updated December 15, 2003, Question 18.

[25] *See also* NASD Anti-Money Laundering Frequently Asked Questions, Updated December 15, 2003, Question 21.

[26] NASD Manual, Conduct Rule §3110 (formerly known as the Rules of Fair Practice), which requires that, for each account open, the firm must maintain certain information, including (i) the customer's name and residence; (ii) whether the customer is of legal age; (iii) the signature of the registered representative (broker) introducing the account and the signature of the member or partner, officer or manager who accepts the account; and (iv) if the customer is a corporation, partnership or other legal entity, the names of any persons authorized to transact business on behalf of the entity. Additionally, for each account other than institutional accounts and accounts in which investments are limited to transactions in money market funds, NASD Rules mandate that each member make reasonable efforts to obtain (prior to the settlement of the initial transaction in the account), the customer's tax identification or social security number, the customer's occupation (including the employer's name and address), and whether the customer is an associated person of another member.

- ξ an address which must be for an individual, a residential or business street address;

- ξ for an individual who does not have a residential or business street address, an army post office or fleet post office box number or the residential or business street address of a next of kin or another contact individual; or

    - o for a person other than an individual, such as a corporation, partnership or trust, a principal place of business local office or other physical location; and

    - o an identification number, which must be:

        - ③ for a U.S. person, a taxpayer identification number; or

        - ③ for a non-U.S. person, one or more of the following: a taxpayer identification number, a passport number and a country of issuance, an alien identification card number, or the number and country of issuance of any other government issued document evidencing nationality or residence and bearing a photograph or similar safeguard.[27]

A broker-dealer must maintain records of all of the identification information obtained from the customer for five years after the account is closed. In addition, records made about information that verifies a customer's identity only have to be retained for five years after the record is made. In all other respects, the records must be maintained pursuant to provisions of §17A-4.[28]

A CIP must include procedures for determining whether a customer appears on any known list or suspected terrorists or terrorists organizations issued by any federal government agency and designated as such by treasury in consultation with federal functional regulators. The procedures must require that the broker-dealer make such determination within a reasonable period of time after the account is open or earlier if required by another federal law or regulation or federal directive issued in connection with the applicable list. The adopting release of Rule 3011 also mentions, as an example, that firms must check the list compiled by the Office of Foreign Assets Control ("OFAC") to ensure that potential customers and existing customers, on an

---

[27] *See* NASD Anti-Money Laundering Frequently Asked Questions, Updated December 15, 2003, Question 23; see also NASD Notice to Members 03-34.

[28] *See* NASD Anti-Money Laundering Frequently Asked Questions, Updated December 15, 2003, Question 35.

ongoing basis, are not prohibited persons or entities and are not from embargoed countries or regions before transacting any business with them.[29]

Rule 3011 acknowledges that there may be circumstances in which a firm may be able to rely on the performance by another financial institution of some or all of the elements of a firm's CIP. Therefore, the final rule provides that a CIP may include procedures specifying when the broker-dealer will rely on the performance by another financial institution (including an affiliate of any procedures of the broker-dealer's CIP) with respect to any customer of the broker-dealer that is opening an account or has established an account or similar business relationship with the other financial institution to provide or engage in services, dealings, or other financial transactions. In order for a broker-dealer to rely on another financial institution, the following requirements must be met:

- reliance must be reasonable under the circumstance;
- the other financial institution must be subject to a rule implementing the anti-money laundering compliance program requirements of the Act and be regulated by a federal functional regulator;
- the other financial institution must enter into a contract requiring it to certify annually to the broker-dealer that it has implemented its anti-money laundering program, and that it will perform (or its agent will perform) specified requirements of the broker-dealer's CIP.[30]

Under Rule 3011 both the introducing firm and the clearing firm are responsible for establishing anti-money laundering compliance programs regardless of the fact that they play differing roles with respect to the customer and have access to different types of customer or activity information.[31] Introducing firms must have a basis for assuring themselves that their clearing firms are monitoring customer account activity on their behalf.[32] Similarly, clearing firms must have a basis for assuring themselves that their introducing firms are following appropriate customer identification procedures. Responsibilities relating to AML compliance should be clearly allocated between the parties, and such responsibilities should be specified in the parties'

---

[29] *See* NASD Anti-Money Laundering Frequently Asked Questions, Updated December 15, 2003, Question 36. *See* www.treas.gov/offices/eotffc/ofac. OFAC periodically publishes a list of "Specially Designated Nationals and Blocked Persons."

[30] *See* NASD Anti-Money Laundering Frequently Asked Questions, Updated December 15, 2003, Question 38; see also NASD Notice to Members 03-34.

[31] *See* NASD Anti-Money Laundering Frequently Asked Questions, Updated December 15, 2003, Question 39.

[32] The NASD has published a Small Firm Template Anti-Money Laundering Program containing compliance and supervisory procedures which is available on the NASD website at www.nasdr.com.

clearing agreements pursuant to NASD Rule 3230. An allocation, however, will not relieve either party from its independent obligation to comply with AML laws.[33]

To enforce compliance with Rule 3011, the SEC and the NASD are including as a part of their periodic inspections (an AML exam) and will be vigorous to insure full AML compliance.[34]

III. Other Entities Deemed Financial Institutions in the U.S.

The term "financial institution" under the Act covers a broad range of financial entities, including investment company. However, officials of the Department of the Treasury, the government department charged with enforcing the Act, are also now seeking to interpret the term "investment company" under the Act broadly to include all forms of investment funds, including private investment funds, such as hedge funds and venture capital funds, not just SEC registered and regulated funds that fall within the definition of investment company under the Investment Company Act of 1940, as amended, such as mutual funds.

A. Mutual Funds[35]

Effective October 1, 2003, the U.S. Department of the Treasury through FinCEN and the SEC adopted a final rule implementing Section 326 of the Act.[36] The final rule, which went into effect on October 1, 2003, requires the adoption of formal anti-money laundering policies, more aggressive know your customer ("KYC") standards, and new record keeping and reporting requirements. Section 326 requires the Secretary of the Treasury and the SEC to prescribe a regulation that, at a minimum, requires investment companies to implement procedures to verify the identity of any person seeking to open an account, to the extent reasonable and practical, to maintain records of the information used to verify the person's identity, and to determine whether the person appears on any lists of known or suspected terrorists or terrorists organizations provided to investment companies by any government agency.

On August 11, 2003, the staffs of the Department of the Treasury and the SEC issued guidance regarding the Mutual Fund Customer Identification Program Rule (31 C.F.R. 103-131). These questions and answers clarify a number of areas. For example, a shareholder of a mutual fund who exchanges his or her shares for a second mutual fund of the same complex is not deemed a customer of the second fund, and therefore, the second fund need not perform customer identification procedures with

---

[33] *See* NASD Anti-Money Laundering Frequently Asked Questions, Updated December 15, 2003, Question 40.

[34] SEC speech, Lori A. Richards, *The Next Phase: Implementing the Patriot Act*, SIA Conference on Anti-Money Laundering Compliance, May 27, 2003.

[35] As used in this chapter, the term Mutual Funds and Investment Company are used synonymously.

[36] SEC 1c-26031, 31 C.F.R. Part 1 of 3.

respect to that shareholder as long as the second fund has a reasonable belief that it knows the true identity of the shareholder. The CIP rule for mutual funds defines a customer of a mutual fund as a person who establishes a "new account" with the fund. "Account" is defined as "any contractual or other business relationship between a person and a mutual fund established to effect transaction in securities issued by the mutual fund including the purchase or sale of securities" (emphasis added). A shareholder who has exchange privileges with other funds has a "business relationship" with those funds to effect transactions in their securities. Thus, the shareholder has an account with the exchanging fund, and the fund may rely on this exclusion from the definition of "Customer."

Assuming that all account opening, share purchase and redemption activities of mutual funds are conducted by either a registered broker-dealer or by the fund's transfer agent, much of the compliance for mutual funds will revolve around making sure that the broker-dealer or transfer agent has taken steps to comply with the anti-money laundering requirements of the Act. However, in any case, mutual funds should also have a written CIP policy setting forth a broad statement regarding the company's policy against money laundering and funding of terrorists or criminal activity. As in the case of an omnibus account with broker-dealers, under the Mutual Fund CIP Rule, a broker-dealer or other intermediary who opens accounts with mutual funds through the NSCC Fund/SERV system, including sub-accounts for individual customers of the broker-dealer, would be the person who opens the new account and would therefore be the customer under the CIP rule, and the broker-dealer/intermediary's customers would not be deemed to be customers of the mutual fund under the Mutual Fund CIP Rule.

B. Private Investment Funds, Hedge Funds, Commodity Pools, and REITS

On September 26, 2002, FinCEN published a proposed rule which would amend the Bank Secrecy Act to prescribe certain minimum standards for unregistered investment companies, such as hedge funds, commodity pools, real estate investment trusts, and similar investment vehicles pursuant to the revised provisions in the Bank Secrecy Act that requires financial institutions to establish anti-money laundering programs.[37] However, these proposed rules have not as yet been enacted.

Unless affiliated with a registered broker-dealer, private investment funds, such as venture capital funds, hedge funds, and commodity pools, it is recommended that these entities require the adoption of a policy statement, designation of a compliance officer for money laundering and the implementation of more formalized and enhanced KYC procedures.[38]

---

[37] 67 FR 187 (September 26, 2002).

[38] The compliance officer can develop an awareness of recent developments, techniques, and trends by visiting the websites maintained by and review publications by Financial Action Task Force (FATF). See www1.oecd.org/fatf and the Financial Crimes Enforcement Network (FinCEN). As recently as January

For each investor of the fund's KYC, compliance procedures would consist of the gathering of at least the following information:

For Individuals:

- ξ full legal name, address and citizenship;
- ξ social security number; and
- ξ signature.

For entities:

- ξ official legal name and address;
- ξ name and signature of an authorized representative;
- ξ tax i.d. number;
- ξ if the investor is a trust, identify the principal owners of the trust and obtain information regarding the authorized activities of the trust and persons authorized to act on behalf of the trust;
- ξ establish internal processes for verifying identities of non-U.S. citizens, foreign corporations or entities established or located outside the U.S.; and
- ξ cross-reference the names of new and existing investors against the list of Specially Designated Nationals and Blocked Persons maintained by OFAC.[39]

This procedure should also be undertaken whenever there is a transfer of an interest or the investor changes his name.

There should also be a focus on individuals or entities residing in or located in certain countries or regions identified by recognized international organizations or other

---

2004, the following countries were listed as non-cooperative: Cook Islands, Egypt, Guatemala, Indonesia, Myarmar, Nauru, Nigeria, Philippines, and Ukraine. A number of countries were removed from the FATF list in 2002 and 2003, including the Bahamas, Cayman Islands, Liechtenstein, St. Kitts, Nevis, and Panama. *See* www.fincen.gov.

[39] *See* www.treas.gov/offices/eotffc/ofac. OFAC periodically publishes a list of "Specially Designated Nationals and Blocked Persons." *See infra* note 29.

groups as non-cooperative with international anti-money laundering principals or procedures or having inadequate anti-money laundering measures. Such agencies include the FATF and FinCEN.

C. Registered Investment Advisers

On April 28, 2003, FinCEN, and the Department of the Treasury, proposed an AML rule for registered investment advisers.[40] However, at this time final rules have not been adopted. On February 12, 2004, the SEC issued a no-action letter through the Securities Industry Association which provides that broker-dealers be permitted to treat registered investment advisers as if they were subject to an AML rule for the purposes of the broker-dealer customer identification rule, provided that all other requirements and conditions in paragraph b(6) of the CIP rule are met, namely that (1) such reliance is reasonable under the circumstances, (2) the investment adviser is regulated by a federal functional regulator (in this case the Division of Investment Management of the SEC, for example), and (3) the investment adviser enters into a contract requiring it to certify annually to the broker-dealer that it has implemented an anti-money laundering program and that it will perform (or its agent will perform) specified requirements of the broker-dealer's customer identification program.[41]

IV. Non-U.S. Banking Implications

In addition to the prohibition on correspondent accounts with foreign shell banks as described in Section IIB. herein, Section 311 of the Act authorizes the Secretary of the Treasury, subject to certain requirements of consultation with senior government officials, with the discretion to impose upon financial institutions special measures with respect to certain foreign jurisdictions, foreign financial institutions, classes of international transactions and account types designed to be of "primary money laundering concern to the United States." Where a financial institution may be interacting with such an institution or jurisdiction or avails itself of such account types or transactions, the Secretary of the Treasury can impose a number of special measures, which include (1) requirements of additional record keeping or reporting, (2) identification of foreign beneficial owners of certain accounts at a United States financial institution, (3) identification of foreign bank customers who use an interbank payable-through account opened by that foreign bank at the United States bank, (4) identification of foreign bank customers who use an interbank correspondent account opened by that foreign bank at a United States bank, and (5) restriction or prohibition of the opening or maintenance of certain interbank correspondent or payable-through accounts. While no special measures have been announced by the Secretary of the Treasury to date, affected financial institutions may in the future be subject to additional administrative and other duties in order to meet these compliance requirements.

---

[40] 68 F.R. 23646 (May 5, 2003).

[41] This no-action letter position shall be withdrawn without further action on the earlier of (1) the date upon which the AML rule for advisers becomes effective, or (2) February 12, 2005.

V. Information Sharing and Potential Liability

Foreign financial institutions involved in securities or other investment activities must be mindful of the interplay between the Act and their own bank's secrecy laws. The Act requires some fairly broad disclosure of what may be confidential information, potentially in violation of compliance procedures and other state and federal privacy laws. Many institutions fear that the disclosures required under the Act could result in disclosure to the public through the Freedom of Information Act ("FOIA") requests. Such fears are not unfounded. The banking, hedge fund, and securities industries depend upon confidentiality and advertise such benefits. Enactment in the last few years of laws and regulations related to privacy as well as private lawsuits for failure to maintain such privacy have risen in the last several years. Under the Act, with respect to disclosures of business records to law enforcement agencies, there are numerous express statutory limitations on liability. Additionally, the FOIA provides certain exemptions from requests that may cover the types of information voluntarily provided to the U.S. government. Exemption 2 of FOIA provides protection from disclosure for information "related solely to internal personnel rules and practices of an agency." Exemption 4 of FOIA provides for maintaining the privacy of disclosures under the Act, as it protects from disclosure of "trade secrets and commercial or financial information obtained from a person and privileged or confidential." In addition, information provided pursuant to reports under the Act may also be shared among other federal and state agencies. Nonetheless, disclosure of such information does pose a potential minefield for financial entities.

VI. Penalties for Non-Compliance

Violations of the Act can result in civil penalties of up to $1 million per violation as well as criminal sanctions of up to 20 years. Violations of the rules issued by OFAC can result in civil money penalties of up to $5 million and criminal sanctions of up to 30 years.

It is unclear at this point whether there may in fact be a private right of action under the Act, the Bank Secrecy Act, or pursuant to other applicable state or federal laws for violations by financial institutions which ultimately lead to the financing of terrorism. While the matter is not free from doubt, it is clear that strong vigilance on the part of affected entities is required to minimize potential liability as the potential for catastrophic liability exists.

VII. Comparison with Selected International and Swiss Regulations

A. International Developments

Over the last years, several international organizations have developed important standards in the fight against money laundering. Compliance with such standards has become the object of regular controls by international experts, such as

the mutual evaluation procedures of the FATF[42] or the Financial Assessment Programs of the International Monetary Fund[43]. It is therefore increasingly relevant to take international regulations into account while analyzing or construing domestic rules.

Among the most significant international instruments adopted recently are the following:

(1) The FATF 40 Recommendations

Today, most OECD countries are members of the FATF. The 40 recommendations were initially enacted in July 1989 and amended in June 1996. They have been thoroughly reviewed and updated in 2003 to incorporate recent developments and now apply not only to money laundering but also to terrorist financing. The recommendations form internationally recognized minimum standards to effectively combat money laundering and terrorist financing. In an additional response to the September 11, 2001, events, they have recently been completed by the Eight Special Recommendations on Terrorist Financing, as part of the international coordination efforts to prevent the misuse of the international financial system by terrorists. The recommendations define minimum requirements for financial institutions, such as undertaking appropriate customer due diligence measures, including identification and verification of the customers' identity. These obligations also require the identification of the beneficial owner, i.e, the natural person who ultimately owns or controls a customer or the person on whose behalf a transaction is being conducted, as well as the individual who exercises the ultimate effective control over a scheme or arrangement.[44] Additional due diligence rules have been introduced in connection with so-called politically exposed persons ("PEPs"), that is persons who have been entrusted with prominent political functions in a foreign country, including their family members or close associates. The recommendations also contain provisions on the record keeping obligations of financial intermediaries, on the special attention that must be paid to complex or unusual transactions and the necessity to review their legal and economic background, as well as on the duty to report suspicious transactions (where a financial institution has reasonable grounds to believe that funds are the proceeds of a criminal activity or are related to terrorist financing.

(2) The International Monetary Fund Financial Assessment Programs

The International Monetary Fund ("IMF") has developed a special methodology and formulated a certain number of criteria to evaluate the compliance and the implementation of the relevant anti-money laundering international standards such

---

[42] *See infra* note 14.

[43] *See* www.imf.org/external/np/fsap/fsap.asp.

[44] *See* Glossary attached to the 40 FATF Recommendations.

as the FATF recommendations.[45] Through this system, the IMF reviews and analyzes the anti-money laundering arsenal of different countries.

(3) The FATF Special Recommendations of Terrorism Financing

In October 2001, the FATF adopted in Washington a program that must be immediately complied with by all world nations. These new recommendations have in particular extended the duty to report suspicious transactions to terrorism financing and introduced the duty for financial institutions to identify the customer (the originator) by providing its name, address, and account number) in all international wire transfers. Financial intermediaries must additionally ensure that non-profit or charitable entities or organizations cannot be misused as conduits for terrorist financing.

(4) International Convention for the Suppression of the Financing of Terrorism

Ratification of this international treaty, which was adopted on December 9, 1999,[46] constitutes one of the FATF Special Recommendations on Terrorism Financing. In addition to defining terrorism financing, this convention tends to foster the international cooperation in the fight against terrorism financing as well as to prevent the preparation and the implementation of financial activities related to terrorism.

(5) Wolfsberg Principles

The Wolfsberg Group[47] is a private association of twelve global banks that decided to develop their own minimum standards for KYC, anti-money laundering, and counter-terrorist financing policies. The principles constitute an interesting soft-law contribution to the international body of anti-money laundering, not only particularly because they are based on a differentiated approach to risk (meaning that large legal and reputational risks require more extensive due diligence procedures), but also because the members of the Wolfsberg Group, who represent more than fifty percent of the worldwide private banking activities, have committed to apply these principles globally, i.e, not only at home, but also in all their branches and subsidiaries, including their offshore entities. Taking into consideration the size of the financial institutions involved, it can be expected that the Wolfsberg principles will have an impact on proposed national legislations in this area.

---

[45] Fund and Bank Methodology for Assessing Legal, Institutional and Supervisory Aspects of Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT Methodology) 2002.

[46] International Convention for the Suppression of the Financing of Terrorism, A/RES/54/109; http://www.untreaty.un.org/English/Terrorism/Conv12.pdf.

[47] http://www.wolfsberg-principles.com. The Wolfsberg Group is composed of ABN Amro Bank N.V, Banco Santander SA, Bank of Tokyo-Mitsubishi Ltd, Barclays, Citigroup, Credit Suisse Group, Deutsche Bank AG, Goldman Sachs, HSBC, J.P Morgan Chase, Société Générale, UBS AG.

(6) Customer Due Diligence Paper of the Basle Committee

The Basle Committee[48] adopted in October 2001 its own set of minimum standards on KYC policies that should apply to bank in all countries.[49] This document aims at reviewing the area of KYC rules from a wider prudential perspective of risk management. According to the Basle Committee, sound KYC policies and procedures are necessary to protect the safety of banks and the integrity of the banking system as a whole. This paper for the first time formally enshrines the principle of a differentiated approach to risk, which has then been taken over by other forums (like the Wolfsberg Group): higher risk relations or transactions require higher standards of due diligence. According to the Basle Committee, banks that aim to attract high net worth individuals must apply enhanced diligence. This is the formal acknowledgment that private banking involves special risks and requires specific skills and expertise. Banks and other financial institutions are required by the Basle Committee to develop clear customer acceptance policies and procedures. Banks and other financial institutions with branches or subsidiaries abroad must define and manage their legal, operational, reputational and concentration risks on a global and consolidated basis. Where the minimum KYC standards differ from one jurisdiction to the other, branches and subsidiaries must apply the higher standards of the two.

(7) Supervisors' PEP Working Paper 2001

Following the November 2000 conference held in Lausanne by representatives of judicial and banking authorities of the G-7 and of Switzerland, recommendations were elaborated concerning the acceptance by financial institutions of funds of individuals with prominent political functions.[50]

(8) European Union Directive Against Money Laundering

In 1991, the European Union enacted its first directive on money laundering, which was updated and extended in 2001.[51] Whereas, the 1991 directive was limited to the combat against laundering the proceeds of drug trafficking, the new directive obliges Member States to combat the laundering of the proceeds of a whole

---

[48] The Basle Committee was created in 1974 by the governors of the central banks of the G-10 at the Bank for International Settlements in Basle, Switzerland. The Committee includes representatives from central banks and financial regulators from the following countries: Belgium, Germany, France, Italy, Japan, Canada, Luxembourg, the Netherlands, Sweden, Switzerland, Spain, the United Kingdom and the USA.

[49] Customer Due Diligence for Banks; http://www.bis.org/publi/bcbs85.htm.

[50] Supervisor's PEP working paper 2001; this document can for instance be found on the Swiss Federal Banking Commission's website at http://www.ebk.admin.ch/f/aktuell/neu090702-03f.pdf.

[51] Directive 2001/97/EC of the European Parliament and of the Council of 4 December 2001 amending Council Directive 91/308/EEC on prevention of the use of the financial system for the purpose of money laundering, OJ L 344, 28/12/2001, p. 0076-0082 (http://europa.eu.int/eur-lex/pri/en/oj/dat/2001/l_344/l_34420011228en00760081.pdf.

series of underlying offenses. The directive further imposes obligations on the reporting of suspicious transactions. To ensure the fullest possible coverage of the financial sector, it applies not only to banks, but also to all other kinds of investment firms, including brokers, mutual fund managers, and independent asset managers, as well as insurance companies. Notaries and lawyers may fall within the scope of the directive when participating in financial or corporate transactions. Same thing for external accountants, auditors, real estate agents, art dealers, casinos, etc. The directive further contains several provisions on customer identification and report-keeping obligations.

(9) Other International Instruments

Many other international treaties exist in the field of the fight against money laundering and related issues. Introducing each of them would certainly exceed the scope of this contribution. Among the most important documents, we should mention the United Nations Convention against illicit traffic in narcotic drugs and psychotropic substances,[52] the Convention on Laundering, Search, Seizure and Confiscation of Proceeds of Crime,[53] the OECD Convention against Bribery of Foreign Public Officials in International Business Transactions of November 21, 1997,[54] the Council of Europe Criminal Law Convention on Corruption of January 27, 1999,[55] and the United Nations Convention against Transnational Organized Crime of November 15, 2000.

B. Switzerland

As in the U.S., the Swiss legal framework relating to the fight against money laundering has rapidly evolved during the last decade. It has now been considerably tightened over the last years. Several new acts and regulations have been passed, both at the criminal and at the regulatory levels. As an important financial centre, Switzerland has been devoting considerable energies and resources to prevent and combat money laundering. The Swiss legal system has recently been found to be compliant with the international standards described above by international experts of the IMF within the framework of the Swiss Financial Assessment Program.[56] Specific provisions were introduced in the Swiss Criminal Code in 1990 to penalize money

---

[52] http://www.incb.org/e/ind_conv.htm.

[53] http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=141&CM=8&DF=07/05/04&CL=ENG

[54] http://www.oecd.org/document/21/0,2340,en_2649_34859_2017813_1_1_1_37447,00.html.

[55] http://conventions.coe.int/Treaty/en/Treaties/Html/173.htm.

[56] It can be reminded here that Switzerland is a member of Interpol, is one of the founding members of the FATF, has ratified several international bilateral and multilateral agreements in which it has committed itself to provide mutual assistance in criminal matters, such as the European Convention on Mutual Assistance in Criminal Matters, has ratified the Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime of November 8, 1990, and has signed the UN Convention against Transnational Organized Crime.

laundering, on the one hand, and lack of care in financial matters, on the other. In 1997, the Money Laundering Act was adopted to establish minimum standards of due diligence and organization for all financial intermediaries in Switzerland. On December 18, 2002, the Swiss Federal Banking Commission ("FBC")[57] enacted the Money Laundering Ordinance that applies to banks, securities dealers, investment fund managers, and other regulated intermediaries to further prevent acts of money laundering.[58] The Swiss Bankers' Association also promulgated its own self-regulatory standards for the banking industry: the Swiss Agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence ("CDB 03") of February 10, 2003.[59] Other financial intermediaries who are not subject to the supervision of the FBC must comply with different sets of rules and standards, promulgated either by specific self-regulatory organizations (like the Swiss Asset Managers Association) or by the Federal Money Laundering Control Authority.[60]

C. Criminal Code

Article 305bis of the Swiss Criminal Code punishes with imprisonment[61] or fine any individual who carries out an act that may prevent determining the origin of, the discovery of, or the confiscation of assets that, as he knows or should assume, stem from a crime. In severe cases, the sanction is prison for up to five years, and it can be combined with a fine of up to CHF 1 million. Article 305bis thus refers to assets that stem from a crime. It can be any crime, whether committed in Switzerland or abroad, and covers offenses like fraud, including tax fraud, forgery, drug trafficking, and bribery of Swiss or foreign officials. If the original crime has been committed abroad, it must be punishable both in the country in which it was committed and in Switzerland.

Pursuant to Article 305ter of the Swiss Criminal Code, any individual who, on a professional basis, accepts deposits, invests, or assists in the transfer of assets from third parties without verifying the identity of the beneficial owner of such assets with the due care required under the circumstances may be punished by up to one year of imprisonment or by a fine. Under this provision, the mere fact that the financial institution neglected to identify with due care the beneficial owner of the assets is sufficient to render him punishable even if the assets are not of a criminal origin. The standards of due care required under the circumstances are not defined in the criminal code, but can be found in other texts, such as the Swiss Bankers' Association CDB 03.

---

[57] http://www.ebk.admin.ch.

[58] The FBC's Money Laundering Ordinance replaces previous circulars against money laundering issued by the FBC in 1991 and 1998.

[59] The CDB 03 replaced a previous version of the Agreement that had been adopted in 1998. The first code of conduct had been adopted by the FBC as early as 1977.

[60] http://www.gwg.admin.ch/f/index.htm.

[61] According to Article 36 of the Swiss Criminal Code, imprisonment means jail of between three days and three years.

Other provisions of the Swiss Criminal Code may come into consideration, directly or indirectly, in the combat against money laundering and terrorism financing, such as Article 260ter (criminal organization), Article 58 and ff. (confiscation) and the recently adopted Articles 100quarter and art. 100quinquies on corporate criminal liability, that came into force on October 1, 2003.

D. The Money Laundering Act

The Money Laundering Act of October 10, 1997, supplements the above-mentioned Articles of the Swiss Criminal Code. It applies to all financial intermediaries, whether subject to the supervision of the FBC or not. This includes banks, securities dealers, mutual funds managers, hedge fund managers, independent asset managers, precious metal dealers, lawyers, and any other person, who, on a professional basis, accepts, holds in deposit, invests, or transfers third parties' assets. Its scope of application is thus very broad and covers both the banking and the non banking-sectors.

The Money Laundering Act further defines the due diligence obligations of all financial intermediaries. These obligations are the following:

- *duty to verify the identify of the customer* (the customer must be identified on the basis of his passport, identity card or similar document upon establishment of the relationship. The financial intermediary must gather all relevant information, to his full satisfaction, on the customer's name, surname, date of birth, citizenship and private address)[62];

- *duty to identify the beneficial owner* (the person who ultimately controls the assets must be identified if the customer is not the beneficial owner or if there is a reasonable doubt in this respect, if the customer is a so-called domicile company, that is a company with no commercial activities, and if an important cash transaction is carried out)[63];

- *duty to renew these verifications* in the course of the relationship if any doubt arises;

- *duty to clarify the economic background* and objective of a transaction or of a relationship when they appear unusual or when there is any element tending to show that the assets might stem from a crime or otherwise be connected with a criminal organization (including a terrorist organization);

---

[62] If the customer's identity has not been verified upon establishment of the relationship, it must be ascertained whenever a cash transaction is executed, in one or several connected transactions, on an amount exceeding the threshold set by the competent authority (e.g., CHF 5,000.- for financial intermediaries subject to direct surveillance of the Federal Money Laundering Control Authority or CHF 25,000.- for banks).

[63] *See infra* note 61 in this respect.

- *duty to keep proper records* of all transactions and relationships (paper-trail obligation). Banks must undertake regular reviews of existing records. All documents must be kept for a period of ten years after the end of the transaction or of the relationship;

- *duty to take appropriate organizational measures* to deter and prevent money laundering. Financial intermediaries must in particular educate their employees and carry out regular controls of their organization and procedures.

Under the Money Laundering Act, financial intermediaries must also file a report with the Money Laundering Reporting Office if they know or should assume that the assets involved in a transaction or relationship stem from a crime, belong to a criminal organization or are otherwise connected with an act of money laundering. Failure of filing such report may lead to criminal liability. Upon filing of a report, the financial intermediary must freeze the assets for a period of five days, pending a decision from the competent judicial authorities, and is prevented from informing his customer and any third party about the filing of the report.

E. FBC's Money Laundering Ordinance

The FBC's Money Laundering Ordinance (the "Ordinance"), which applies to all financial intermediaries who are subject to surveillance by the FBC,[64] completes and implements the Money Laundering Act with respect to a certain number of due diligence obligations, such as the duty to clarify the economic background and objective of a relationship or transaction, the duty to keep proper records, and the duty to take appropriate organizational measures. The duties to verify the identity of the customer and of the beneficial owner, as well as to renew these verifications, are regulated by the Swiss Bankers' Association CDB 03.[65]

The Ordinance constitutes the Swiss implementation of the Basle Committee Customer Due Diligence Paper of October 2001.[66] It introduces the concept of a risk-differentiated approach, requiring enhanced due diligence for higher risks. Under the Ordinance, banks and securities dealers are thus required to define two or more risk categories as well as the criteria that should apply to allocate each customer to a specific risk category. The following criteria are proposed by the Ordinance to assign customers to a higher risk category: the customer's country of domicile, citizenship, or origin (e.g., FATF or non-FATF countries), the nature of the customer's professional or commercial activities, the lack of meeting between the bank and the customer (relationship established by correspondence), the size of the customer's

[64] That is, banks, securities dealers and investment fund managers. Other financial intermediaries are subject to other analogous regulations issued either by the Federal Money Laundering Control Authority or by self-regulatory organizations.

[65] *See* next Section.

[66] *See infra* note 48.

assets, etc. Politically exposed persons (so-called PEPs) belong in any event to the higher risk category. The establishment of a banking relationship with a higher risk customer requires approval by the bank's manager or even by the bank's highest management (CEO), for instance for PEPs. Enhanced due diligence requirements apply to all customers who have been allocated to the higher risk category. For this kind of customer, banks must draw a detailed client profile and ascertain whether the customer is the beneficial owner of the assets, the origin of the assets (as well as of the customer's income and wealth), the intended use of the funds, the customer's professional or commercial activities, etc. These verifications, and their plausibility, must obviously be properly documented. The Ordinance further reiterates that banks are prohibited from accepting assets that they know, or should assume, are the proceeds of criminal activities, committed in Switzerland or abroad. The proceeds of criminal activities clearly include assets deriving from bribery, embezzlement of public funds, or abuse of an official function. The same bar applies on any kind of business relationship with individuals who, the bank should know or presume, are affiliated in any way whatsoever with a terrorist or criminal organization.

Under the Ordinance, financial intermediaries are also required to set up effective procedures for monitoring transactions. They must introduce computer systems to facilitate the detection of higher risk transactions.

Swiss financial intermediaries with branches or subsidiaries located outside Switzerland are required to identify, manage, and control the legal, operational, and reputational risks associated with money laundering or terrorism financing on a global basis. Banks active internationally must accordingly ensure that the group's internal and external auditors are able to access information concerning specific business relationships, if needed. Group companies must supply to the head office the information necessary for such global risk management.

Banks must of course adopt appropriate internal codes of conduct or compliance guidelines to properly organize themselves. Such documents must set out the criteria to be applied in identifying higher risk relationships or transactions, the procedures to identify, manage, and control the risks, the principles of the transaction monitoring system, the internal competent anti-money laundering bodies, the staff training principles, the corporate policy on PEPs, the different internal responsibilities, etc.

F. Swiss Bankers' Association Agreement on the Swiss Banks' Code of Conduct with Regard to the Exercise of Due Diligence (CDB 03)[67]

This document was adopted for the first time in 1977 by Swiss banks as a private code of conduct. It has been amended several times since then and has now become an essential piece of the Swiss anti-money laundering arsenal. It has even served as a source of inspiration for the FATF 40 Recommendations and, to a certain extent, the Basle Committee Customer Due Diligence Paper. It is now part of the

[67] http://www.swissbanking.org/en/1116_e.pdf.

mandatory rules with which Swiss banks, including Swiss branches of foreign banks, must comply. The bank's statutory auditors are required by the FBC to monitor compliance with the CDB 03, and serious breaches of the CDB 03 may cause financial intermediaries to no longer meet the fit and proper conduct requirement (in addition to being fined to up to CHF 10 million). The core minimum standards of the CDB 03 consists of rules on the identification of customers and beneficial owners, as well as on the renewal of the verifications as an on-going obligation in the course of the relationship. It thus implements part of the Money Laundering Act, as well as "*the due care that can be reasonably expected under the circumstances*" (see Article 305ter of the Swiss Criminal Code).

Under the CDB 03, banks must verify the customer's identity when establishing a business relationship with said customer. This applies to:

- the opening of cash, securities or deposit accounts;
- the entering into of fiduciary transactions;
- the renting of safes;
- the conclusion of management agreements for assets deposited with third parties; and
- the execution of any transaction, including cash transactions, exceeding CHF 25,000.-

The bank must verify the customer's identity by examining and keeping a copy of an official identification document with a photograph and put on record the customer's full name and surname, date of birth, citizenship, and address of domicile, as well as the means used to verify the identity. Special provisions apply for legal entities. Banks must additionally establish the identity of the beneficial owner, that is of the person who ultimately controls the assets, irrespective of the legal characteristics of the relationship between the customer and the beneficial owner, with all due diligence which can reasonably be expected under the circumstances. Banks must require from the customer, by means of the famous so-called Form A, a written declaration setting forth the identity of the beneficial owner. Should the customer enter false information in Form A, he may become criminally liable under Article 251 of the Swiss Criminal Code (forgery of documents) and be sentenced to up to five years of jail.

For domiciliary companies, that is companies without their own premises, without their own staff or with staff that engages solely in administrative tasks, the beneficial owner must be identified in any event. He can be either an individual or an entity carrying out a true commercial or industrial activity, but never another domiciliary company. In the case of entities or associations without specific beneficial owners, such as discretionary trusts, the customer is required to provide information on the

actual settler as well as on the persons who are likely to become beneficiaries. Any curators or protectors must also be indicated.

The internal and external auditors must be in a position to verify that the required identification procedures have been complied with.

G. Swiss Banking Secrecy and the Combat Against Money Laundering

Banking secrecy refers to the duty of confidentiality that banks, their employees or agents must observe with respect to the professional and personal matters of their clients. In any democratic society, protection of privacy constitutes a fundamental guarantee of individual liberty. For bankers, mutual funds or hedge funds managers as well as securities industries, protection of privacy is of course central to their business. In Switzerland, banking secrecy has various legal bases. It is equally protected under contractual, administrative, and criminal law. The criminal law protection[68] was introduced in the Swiss Banking Act in 1934 in particular to provide protection to persons whose persons and property were being threatened by the German upcoming National-Socialist government on political, religious, or racial grounds. Swiss banking secrecy does not provide anonymity to customers: banks of course always know the customer's identity.

The bankers' obligations to maintain banking secrecy has however never been absolute. For instance, the customer may, as owner of the secrecy, at any time release the bank from its confidentiality obligations. Banking secrecy has also always had to give way to other legal obligations. Banking secrecy may accordingly be lifted by requirements of civil law (inheritance law or marital status rules), of administrative law (debt collection or bankruptcy law, regulatory law) and, of course, of criminal law and international mutual assistance law, including administrative assistance. As an example, Swiss branches or subsidiaries or foreign banks may, under certain circumstances, disclose confidential information to their parent company as well as to the competent foreign supervisory authorities. Swiss banks must of course provide all information and documents to the FBC, if required by the latter. The same rule applies to the disclosure of information to the bank's auditors.

Under the Swiss anti-money laundering regulations, banks are under a duty to file a report to the competent authorities every time they know, or should assume, that the assets stem from a crime or are otherwise connected to a criminal organization. The prosecuting authorities in any criminal proceedings may also lift banking secrecy. Additionally, based either on bilateral agreement, such as with the USA, on multi-lateral agreements, or, failing any agreement, on Swiss domestic law, Switzerland generally grants international assistance in criminal matters to foreign countries provided certain requirements are met. As an example, the assistance will only be granted if the act committed abroad qualifies as an offense of a certain

[68] Article 47 of the Swiss Banking Act. For securities dealers, see Article 43 of the Swiss Stock Exchanges and Securities Traders Act.

importance, both abroad and in Switzerland.[69] Finally, the Swiss financial watchdog (the FBC) may cooperate with foreign banking or securities supervisory authorities and, upon request, make available to such authorities non-public information and documents. This is however subject to certain legal requirements: the foreign authorities must use the information received only for the purpose of direct supervision of regulated financial entities, the foreign authorities must be bound by professional secrecy, and they must undertake not to transfer the information and documents to other authorities unless the FBC has given its prior approval or an international treaty expressly authorizes them to do so.

As a conclusion, it can be noted that Swiss banking secrecy does not at all constitute an obstacle to an efficient fight against money laundering or terrorist financing or, under a broader perspective, against the global combat against international organized crime. It could on the contrary be viewed as a demonstration that the fight against illegal financial activities can be reconciled with the fundamental right to privacy. This balance requires however from financial institutions that they take seriously their due diligence obligations and continually update their systems and procedures to make sure that, at the end of the day, they effectively know their customer and document their knowledge. But is this knowledge not the very heart of any financial activity? Appropriate knowledge of their customers allows financial institutions to offer them the right products and services. Maybe the additional burden placed on financial intermediaries over the last decade could eventually result in a commercial chance.

VIII. Future Rule Making and Trends

Several provisions of the Act, most of which relate to Title II of the Act involving enhanced foreign intelligence and law enforcement surveillance authority, will expire on December 31, 2005. However, the provisions of the amendments to the Bank Secrecy Act facilitated by the Act and certain other provisions discussed in this article will remain in effect far beyond this sunset provision. It is also likely that future acts of terrorism and the ever-changing methods employed to finance such activities will lead to the enactment of further federal and other administrative and legislative rule making and compliance procedures.

Financial institutions must continue to be ever vigilant to meet the compliance and reporting obligations imposed by the Act as well as future legislation and rule making. Many of the largest financial institutions are now deploying proprietary software and powerful internet search tools to assist them in their AML and KYC, such as Web Fountain.[70] Financial institutions must demand effective up-to-date monitoring systems and have clear lines of responsibility for maintaining these systems.

---

[69] Whereas, tax fraud qualifies in principle for international criminal assistance, mere tax evasion does not. Tax fraud involves the use of forged documents or other qualified fraudulent behaviors; whereas, tax evasion is defined as the mere non-disclosure of taxable income or assets.

[70] Brian Hindo, *Citi Scours Deep for Dirty Money*, BusinessWeek, April 5, 2004.

It is clear that a fundamental transformation is taking place in the area of financial transactions worldwide in order to combat the financing of terrorism and other criminal activity. All traditional and non-traditional financial institutions will have to continually be on the lookout for suspicious activity in order to protect both the public as well as to minimize their own exposure as conduits of illegal financing activities. The regulatory environment will continue to evolve as the Department of the Treasury and other regulatory agencies implement additional regulations under the Act. It is also likely that, in the not too distant future, FinCEN will finalize its proposed regulations for hedge funds, commodity pools, private investment funds, and investment advisors substantially along the lines proposed by FinCEN in 2002 and 2003. In this environment, financial entities must continue to not only balance the regulatory requirements, but also their relationship with their customers.

International criminality and terrorism financing have become global and cannot be combated efficiently by any one country alone. International rules and regulations must be adopted and implemented worldwide if democracies want to fight them with success. Additionally, implementing state-of-the-art rules and compliance programs involves considerable costs and may, taking into consideration the threat that they represent to privacy, lead to competitive disadvantages in a borderless financial world. It is therefore crucial that all the financial centers around the world continue coordinating their efforts and resources in this respect and establish a level playing field.