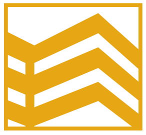

OFFSHORE BANKING TODAY
The Shift From Secrecy To Disclosure

In the recent past, it was not uncommon to include offshore banking services as part of an integrated asset protection plan. The offshore aspect was regarded as particularly attractive to individuals seeking greater privacy and confidentiality in their financial affairs, and the potential tax savings added to its appeal as well. But these protective practices of yesterday are no longer a guaranteed option in today's world. The element of confidentiality has been severely curtailed in most foreign banking transactions for important reasons.The growing threat of global terrorism, recent money laundering scandals, andc ontroversy surrounding many of the popular offshore tax havens have made it all but impossible to avoid some level of disclosure in opening a foreign bank or securities account.

There are several global initiatives – some new and some ongoing –that are rapidly changing the banking landscape. In particular, the **Financial Action Task Force** (FATF), its parent organization – the **Organization for Economic Cooperation and Development** (OECD), and the **Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism Act** of 2001 (the USA Patriot Act) have been instrumental in promoting unprecedented transparency in the banking industry. This article will briefly address the impact of these initiatives on bank secrecy and general client confidentiality issues.

FATF

So what is FATF, and why does it concern you? Formed in 1989, the **Financial Action Task Force on Money Laundering** (FATF) is an inter-governmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat "money laundering."[1] Although an organization with 31 member states, FATF's influence is felt worldwide. FATF's work revolves around the so-called Forty Recommendations it initially adopted in 1990. These recommendations are mainly directed at the criminalization of money laundering activities, the promotion of stricter record keeping requirements for financial institutions, and the development of better control and supervision system for these institutions.

FATF successfully established the Financial Intelligence Units, to facilitate financial information sharing among 58 countries. FATF also blacklisted 15 countries for their refusal to cooperate in the information-sharing initiative.[2] More recently, in the wake of the events of September 11th, FATF developed several Special Recommendations with the aim of denying terrorists access to the international financial system. Among other things, these new recommendations call for strengthening the banking industry's customer identification measures and freezing and confiscating terrorist assets. Together with already existing initiatives, these proposed measures have resulted in much more detailed due diligence requirements[3] for opening a foreign bank account.

Over the years, FATF has worked closely with other international organizations, including the Basel Committee of the **Bank for International Settlements** (BIS). BIS is an international organization, which fosters international monetary and financial cooperation and serves as a prime counterparty for central banks in their financial transactions. Historically, BIS has cooperated with FATF to develop better reporting and customer identification mechanisms within the international banking system.

Within the BIS, the Basel Committee has been particularly aggressive in promoting sound supervisory standards worldwide. Last year, the Basel Committee issued a renewed call for better "Know Your Customer" standards, which emphasize the importance of full disclosure in financial dealings.

In particular, the Basel Committee urges banks to pay special attention to the trust, nominee, and fiduciary accounts, as well as accounts opened in the name of corporate entities and remote or electronic banking accounts. While the Committee acknowledges the importance of confidentiality in certain banking relationships, it nevertheless encourages banks to request identification from all parties involved, mandate certification of relevant personal and corporate documentation, and generally establish to the bank's satisfaction that the account is being opened for legitimate business reasons.

Although actual due diligence requirements vary somewhat from jurisdiction to jurisdiction and bank to bank, the Know Your Customer requirements promulgated by the Basel Committee give banks a wide latitude of actions to verify a customer's identity and validate the purpose of a foreign bank account.Typically, a bank will request the following information before opening an account:

1. Name, address, date of birth, profession, contact information.
2. Details about your banking needs (account currency, amount of deposit, standard transactions you will require, preferred language, etc.).
3. An accurate description of the economic origin of your funds to comply with anti-money-laundering laws.
4. An authenticated (notarized) copy of your passport including the photo page (N.B. –a driver license is usually insufficient)
5. A recent utility bill (water, gas, or electricity–but not telephone) to validate your legal address.
6. If you are paying by credit card, a copy of the card's most recent statement.
7. Additionally, any documents necessary to substantiate your economic background. Although here the documentation varies, some of the more widely requested documents are a copy of your employment contract, university diploma, an updated C.V., etc.).

If the bank account is being opened in the name of a trust, the bank may also require supplemental information, such as the trust deed, identification papers for the grantor(s) and

beneficiaries, as well as other relevant documentation. Similarly, if the account is being opened fora corporate entity, incorporation documents, by-laws, and information about officers and directors will be required documentation specified in the due diligence list.

OECD

The parent body of the FATF, the **Organization for Economic Cooperation and Development** (OECD) is comprised of 30 member countries. Throughout its history, OECD has become increasingly involved in many burning socio-political and economic issues in its pursuit of democratic government and market economy. Many perceive the OECD as the embodiment of the collective will of the industrialized world, forcing its policies upon the smaller, lesser-developed countries. Indeed, OECD has been very aggressive in the international arena, particularly in the area of taxation, leading a multilateral attack on offshore tax havens. OECD's influential 1998 report on Harmful Tax Competition severely criticized the tax policies of no-tax and low-tax jurisdictions, citing increasing flight of capital from high-tax, OECD member countries.

While the aim of theses efforts was blatantly self-serving in advancing the interests of highly developed, industrialized countries, OECD was pivotal in promoting financial information sharing and greater transparency in international banking. Beginning in 2000, OECD targeted over 40 countries deemed tax havens. Although reluctant at first, within 2 years most of the countries pledged their cooperation, fearing the threat of economic sanctions.[4]

Today, OECD continues its attack on offshore tax havens. In particular, in its recent report on Improving Access to Bank Information for Tax Purposes, OECD proposed the ideal level of access to banking information for the purposes of more efficient tax administration. It also identified the measures necessary to achieve the proposed level of openness. Key among these was the elimination of anonymous accounts and requirements for identification of bank customers and beneficial owners of accounts.

While Pursuing somewhat different goals than the FATF, OECD has, nevertheless, made an impact in the changing area of banking secrecy. In view of the global economic slowdown and the threat of terrorism, it is likely that OECD will only intensify its efforts to harmonize international taxation and advance information sharing.

PATRIOT ACT

Following the terrorist attacks on September 11th, the US Congress promptly responded with aggressive new legislation aimed at broadening the scope of executive, judicial, and administrative powers to more effectively combat the terrorist threat. The Patriot Act, as it became known, made sweeping changes to the **Bank Secrecy Act** of 1970 (BSA) as well as to the **Money Laundering Control Act** of 1986 (MLCA).

Among the provisions of the Act, Title III, known as the **International Money Laundering Abatement and Anti-Terrorist Financing Act** of 2001 (IMLAFA), was pivotal in imposing substantially more rigorous due diligence obligations on financial institutions. While Title III is fairly long and convoluted, for the purposes of this article we will discuss only those provisions that have a direct impact on transparency in private banking.

Under the old version of the BSA, customer disclosure requirements applied to a fairly narrow range of financial institutions. Title III extended the applicability of such requirements by expanding the definition of financial institutions to include, among others, private banks, investment banks, securities broker-dealers, insurance companies, and various cash processing entities.

Title III also imposed enhanced due diligence requirements for those financial institutions that maintain correspondent accounts[5] for foreign financial institutions and private banking accounts. Specifically with regard to private banking accounts, the law mandates determining the identity of the beneficial owner and the source of the deposited funds as well as better reporting of suspicious transactions to the appropriate authorities.

Within IMLAFA there are also provisions authorizing the US Attorney General or theSecretary of US Treasury to issue subpoenas or summonses6to any foreign financial institution that maintains a correspondent account in the United States. The scope of these record production orders includes records related to the correspondent account, including information maintained outside the United States if it is related to the deposit of funds in question into the foreign bank.

In addition to the expanded subpoena powers, Title III of the Patriot Act grants the Treasury Secretary the power to impose additional record keeping and reporting obligations on financial institutions conducting business outside the United States as well as on clients and transactions from enumerated foreign jurisdictions. Directed at money laundering prevention, these additional obligations, if imposed, would require information about the beneficial owners of suspect funds and transaction details, including identities of participants.

Among other notable provisions, Title III permits financial institutions to share information with each other on countries, individuals, and transactions having potential ties with terrorism,money laundering, or both. Also, for the first time, registered securities brokers and dealers will be required to file Suspicious Activity Reports (SARs). The SAR is a form produced by the US Department of Treasury. It is filed in those instances where a financial institution has reason to know or suspect that its resources or infrastructure are being used to perpetrate fraud,money laundering, or other related illegal activities.

Finally, the Patriot Act imposes a prohibition on select financial institutions7that bans establishing and maintaining a correspondent bank account with any foreign bank that does not have a physical presence in any jurisdiction, unless such a bank (typically referred to as a "shell bank") is affiliated with an actual physical financial institution subject to regulation in its home jurisdiction.

Mounting international pressure and stricter domestic disclosure regimes have made international banking somewhat less desirable from a confidentiality perspective. Nevertheless, while a lot of the tax benefits are vanishing and the veil of secrecy is being lifted, certain foreign banks may still be utilized for asset protection purposes. The difference is that potential customers dealing with a foreign bank should now be prepared to encounter increased scrutiny and document production requests to satisfy the bank's own internal due diligence requirements. However, those bank customers that comply with the local requirements should not expect to draw undue attention if their business is legitimate, or their asset accounts are part of a properly documented and declared asset protection trust.

This informational article is published by Greenberg & Co., Two Corporate Drive - Suite 234, Shelton, CT 06484 USA. We can be contacted via telephone by calling (203) 225-0200. Our website address is: www.greenbergandco.com, and we can also be reached by email at learnmore@greenbergandco.com. Any request for permission to distribute, reprint, or publish this copyrighted material must be submitted to the above address in writing.