Preventing the use of financial institutions for money laundering and the implications for financial privacy

Dr Chat Le Nguyen

Assistant Professor in Law, Fiji National University

Abstract

Purpose: The article discusses the implication of money laundering preventive measures for financial privacy, with the focus on banking secrecy.

Design/methodology/approach: This article, first, sets out the principal measures imposed on financial service providers to prevent money laundering. The interaction between the preventive measures and the desire for financial privacy is then discussed.

Findings: The adequate implementation of the preventive measures is highly important for financial institutions to be secure from money laundering. Nonetheless, the enforcement of these measures is becoming much more intrusive into financial privacy. In practice, financial privacy should be weighted fairly against the objectives of preventive measures.

Key words: Anti-Money Laundering, Banking Secrecy, Financial Institutions, Customer Due Diligence, Record Keeping and Suspicious Transactions.

Paper type: General review

1. Introduction

A set of preventive measures imposed on financial institutions, which aims at uncovering opportunities offered by the legitimate environment to facilitate money laundering, is an important and indispensable part of the anti-money laundering (AML) regime. The key measures include customer due diligence (CDD), record keeping, and reporting of suspicious transactions. These measures have the objectives of deterring and detecting criminals from using financial institutions for laundering the proceeds of crime. The rationale behind the implementation of these measures is that: i) criminals often make use of financial institutions, especially the banking system, as the main intermediaries for money laundering operations; ii) the interaction with the legitimate environment is seen as a "weak point" in the stages of money laundering, at which law enforcement agencies can intervene for deterring and detecting money launderers; iii) the integrity of financial service providers, which contributes significantly to public confidence,

must be protected from money laundering involvement; and iv) nobody in the legitimate environment should profit from criminals.

CDD, record keeping and the reporting of suspicious transactions are provided for in both "hard laws" (e.g., article 7 of the United Nations Convention against Transnational Organised Crime (UN, 2000b) and article 14 of the United Convention against Corruption (UN, 2003)) and "soft laws" (the Financial Action Task Force (FATF) Recommendations and initiatives of other international organizations). It should be noted that the provisions of the "hard laws" are drafted in a general manner since they build on on-going international initiatives to combating money laundering (UNODC, 2004, p. 50), and "States Parties are called upon to use as a guideline the relevant initiatives of regional, interregional and multilateral organizations against money laundering" (UN, 2000b). The relevant initiatives of regional, interregional and multilateral organizations refer in particular to the FATF Recommendations and initiatives of other international organizations (UN, 2000a). In fact, the FATF, in its Recommendations and their revisions, has detailed and developed extensively the preventive measures. Because of that, this article focuses on examining the preventive measures provided for in the FATF Recommendations.

2. Concepts of customer due diligence and know your customer

It appears that the use of terms "Customer Due Diligence" and "Know Your Customer" (KYC) is sometimes confusing. It is necessary to clarify the meaning of these terms through examining the history and the development of these concepts.

The term "due diligence" has its origins in Anglo-American law, particularly in the statutory regulations controlling the capital market in the United States (US) (Picot, 2002, p. 154). Originally the due diligence concept appeared in security laws designed to protect investors. It then has evolved into the systematic and professional investigation of business opportunities and risks during on-going sale negotiations (Picot, 2002, pp. 154-55). It may entail financial, marketing, human resources, legal and tax, environmental and organizational due diligence (Picot, 2002, pp. 155-78). In other words, the object of the due diligence process is to obtain information on and engage in evaluation of the background of a target company including its structure, the capabilities of its employees, its market opportunities and risks (Picot, 2002, p.

178). With regard to CDD, it normally refers to the investigation procedure of a new customer's background conducted by the financial institution prior to doing business with the new customer.

The term "Know Your Customer" and the "KYC guidelines" originated in a legislative report on the US Bank Secrecy Act, but they were not defined in that report and no examples were given to illustrate what KYC means (Mulligan, 1998, p. 2358). Since 1970, the US government has deployed US banks as the principal agencies to track down the proceeds of crime by imposing an obligation to know their customers and to report suspicious transactions (Grant, 1995, p. 227). As a result of this, KYC principles and KYC guidelines have evolved and become ingrained in the US AML regime as tools for banks to: i) prevent criminals from presenting as their legitimate customers; and ii) reveal the illicit nature of a customer's business (Mulligan, 1998, p. 2358).

The FATF and other international institutions (e.g., the Basel Committee on Banking Supervision) have worked intensively on the KYC issue which "is most closely associated with the fight against money laundering" (Basel Committee on Banking Supervision, 2001, p. 2). In 1988, the Basel Committee on Banking Supervision issued the Statement on Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering including the principle of "Customer Identification". It called for reasonable effort by the international banking community to determine the true identity of all customers requesting their services (Basel Committee on Banking Supervision, 1988, p. 3). In 1990, the first version of the 40 FATF Recommendations provided an initiative to combat the misuse of the financial system for laundering the proceeds of drug-related crimes (FATF, 1990). This version and the later revised ones (in 1996, 2003 and 2012) recommend various measures to prevent financial institutions, certain other businesses and professions from involving money laundering. The FATF uses the term "Customer Due Diligence" or "Identification of Customer" instead of "Know Your Customer" to refer to the preventive measures. In 2001, after identifying the deficiencies in a large number of countries' KYC principles for banks (Basel Committee on Banking Supervision, 2001, p. 1), the Basel Committee on Banking Supervision revised the KYC principles to make them more applicable to all countries. In the CDD for Banks, the scope of the Basel Committee's approach to KYC has been expanded with a view to serving not only AML but also the effective management of banking risks. KYC involves more extensive due diligence for higher risk accounts, and includes proactive account monitoring for suspicious activities (Basel Committee

on Banking Supervision, 2001, p. 1). In short, KYC and CDD have been introduced as evolving concepts designed to be adaptable and effective for use in both banks and other financial institutions. These terms do not have a fixed content, and they frequently appear to be used interchangeably. However, CDD is often used to refer to a standard that is broader than KYC (Koker, 2006, pp. 28-29). KYC could be conceived of as the specific CDD standard imposing on banks and other financial institutions the duty to identify their customers.

3. International standards of CDD and record keeping

3.1 The FATF Recommendations

The leading standards of CDD for the purposes of fighting money laundering and terrorist financing have been set out by the FATF. The FATF has amended its recommendations together with a glossary and interpretative notes that define and clarify comprehensively the CDD standards applied to financial institutions.

According to the 2012 FATF Recommendations (Recommendation (R)10(i), (ii), (iii), and (iv)) (FATF, 2012), a financial institution should be required to undertake CDD measures when:

1) Establishing business relations;
2) Carrying out occasional transactions: (i) above the applicable designated threshold (US$/EUR 15,000); or (ii) that are wire transfers in the circumstances covered by the Interpretative Note to Recommendation 16;
3) There is a suspicion of money laundering or terrorist financing; or
4) The financial institution has doubts about the veracity or adequacy of previously obtained customer identification data.

The CDD measures to be taken are as follows (R10(a), (b), (c), and (d)) (FATF, 2012):

a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.

b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions understanding the ownership and control structure of the customer.

c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

The 2012 FATF Recommendations and their interpretative notes especially emphasize the use of CDD in regard to legal persons and arrangements. They recommend that financial institutions should verify and identify any person purporting to act on behalf of the customer, the beneficial owners and the trustee (Interpretive Note to Recommendation (INR) 10, part (B), (C), and (D)) (FATF, 2012). Further, financial institutions should perform enhanced due diligence on higher risk categories of customers, such as Politically Exposed Persons (PEPs). But they also provide that simplified or reduced CDD measures may be applied to lower risk customers, such as financial institutions or public companies under rigorous regulation, government administration or enterprises (INR 10, pars. 16-18, (FATF, 2012)).

The obligation of record keeping requires that financial institutions keep customer identification and records of financial transactions. The database of this information which can be accessible by law enforcement authorities when required is extremely helpful for the investigation and prosecution of money laundering offences. In their investigations, law enforcement bodies normally need to follow the trails of the movement of criminal proceeds, which can be revealed through the records kept by the financial service providers involved. Thus, record keeping can serve a repressive approach effectively.

R11 of the 2012 FATF Recommendations states that:

Financial institutions should maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal activity.

Financial institutions should keep records on the identification data obtained through the customer due diligence process (e.g., copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence, including the results of any analysis undertaken (e.g., inquiries to establish the background and purpose of complex, unusual large transactions), for at least five years after the business relationship is ended, or after the date of the occasional transaction.

Financial institutions should be required by law to maintain records on transactions and information obtained through the CDD measures.

The CDD information and the transaction records should be available to domestic competent authorities upon appropriate authority.

3.2 The Basel Committee on Banking Supervision

As one of the primary requirements in bank supervision, a comprehensive set of standards of CDD for banks has been developed by the Basel Committee on Banking Supervision that contains four basic elements (Basel Committee on Banking Supervision, 2001, pp. 6-14):

1) Customer acceptance policy: This requires banks to develop clear customer acceptance policies and procedures, including a description of the types of customers that are likely to pose a higher than average risk to a bank. Factors, such as customers' background, country of origin, public or high profile position, linked accounts, business activities or other risk indicators should be considered in preparing this policy. More extensive CDD should be required for higher risk customers.

2) Customer identification: Banks should obtain satisfactory information about the identity of a new customer and the purpose of the business relationship. The adequacy of information depends on the type of applicant and anticipated size of accounts. Special requirements of information are required when implementing CDD measures on PEPs and non-face-to-face customers.

3) On-going monitoring of high-risk accounts: Banks should have an understanding of normal and reasonable account activity of their customers so that they can recognize and report suspicious transactions to the competent authorities. This on-going monitoring mainly aims at higher risk accounts.

4) Risk management: The channels for reporting suspicious transactions should be clearly specified for effective communication. The roles of internal audit and employee-training programmes should be emphasized for insuring effective risk management. Bank staff should have an adequate on-going training about CDD procedures. Audit functions should be staffed adequately because internal audit plays an important role in evaluating risk management.

It is noticeable that the very broad definition of "customer" in "Customer Due Diligence for Banks" issued by the Basel Committee in 2001 includes: i) the person or entity that maintains an account with the bank or those on whose behalf an account is maintained (i.e. beneficial owners); ii) the beneficiaries of transactions conducted by professional intermediaries; and iii) any person or entity connected with a financial transaction who can pose a significant reputational risk or other risks (operational, legal and concentration risk) to the bank (Basel Committee on Banking Supervision, 2001, p. 6).

Beside the Basel Committee which has focused on CDD standards for the banking system, other international associations of financial regulators have also specifically defined the CDD standards or the CDD process for banks and other kinds of financial institutions consistent with the FATF Recommendations.

In 2000, the Wolfsberg Group published the Wolfsberg Anti-Money Laundering Principles for Private Banking (revised in 2002 and 2012) which contains the essential global AML guidelines for private banking (Wolfsberg Group, 2012). It sets out the core guidelines in terms of CDD requirements for the client and the beneficial owner (Wolfsberg Group, 2012, pp. 2-3). Additional due diligence is required in some situations, such as business in relation to clients from high-risk countries (which have inadequate AML standards or where there is a high risk of crime and corruption) or business involving public officials.

In 2004, the International Organization of Securities Commission (IOSCO) introduced its Principles on Client Identification and Beneficial Ownership for the Securities Industry, which states that "the CDD process is a key component of securities regulatory requirements intended to achieve the principal objectives of securities regulation, the protection of investors; ensuring that markets are fair, efficient and transparent; and the prevention of the illegal use of the securities industry" (IOSCO, 2004, p. 2). The CDD process should be applied by the authorized securities service providers to: identify their clients and beneficial owners; obtain adequate information about their clients' circumstances and investment objectives; and keep records of this information (IOSCO, 2004, p. 2). Although the main objectives of this process are to prevent securities fraud and market abuse, the application of the CDD process in the securities industry also contributes to the prevention of the illegal use of the securities industry for the purposes of money laundering and the financing of terrorism (IOSCO, 2004, p. 2).

The International Association of Insurance Supervisors (IAIS), in 2003, revised the Insurance Core Principles and Methodology by adding new principles addressing supervisory standards related to Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) (IAIS, 2003). In 2004, the IAIS issued the Guidance Paper on AML/CFT which contains a specific description of the CDD process as core measures against money laundering and financing terrorism (IAIS, 2004, pp. 6-15).

4. Reporting obligation

The effectiveness of a national AML system is essentially dependent on whether the relevant competent authorities have adequate information on the funds and financial transactions to which suspicions of money laundering arise. This information usually comes from three main sources (Thony, 1996, p. 258): i) mandatory reports provided by persons and institutions covered by law; ii) databases available for access (computer databases for the most part); and iii) information exchanged with other AML authorities. Among these sources, mandatory reporting is a crucial prerequisite for an effective AML strategy for a range of reasons. First, money laundering itself is a crime without direct victims. The information provided by institutions and professions, who are commonly vulnerable to money laundering, is extremely critical to the prevention and investigation of money laundering. Second, money laundering is normally accompanied by the carrying out of financial transactions through financial institutions which maintain certain privacy standards. As a result, law enforcement authorities find it difficult to get information about these transactions. Thus, financial institutions should be subject to the mandatory obligation of reporting suspicious funds or transactions.

Under the reporting obligation, reporting entities are required to analyse the funds and financial transactions involved, then assess whether the funds or transactions raise suspicions. These funds or transactions deemed suspicious must then be reported to the competent authorities. R20 of the 2012 FATF Recommendations reads: "if a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, directly by law or regulation, to report promptly its suspicions to the financial intelligence unit (FIU)".

The Wolfsberg Group, in their Wolfsberg AML Principles on Private Banking, refers to "unusual or suspicious transactions" undertaken in the banking system that may include (Wolfsberg Group, 2012, p. 6):

1) Account transactions or other activities which are not consistent with the due diligence file;
2) Cash transactions over a certain amount; and
3) Pass-through/in-and-out-transactions.

It should be stressed that there is no international consensus on the criteria for identifying suspicious transactions. The international instruments leave room for States to set out their own criteria for identifying suspicious transactions.

The onerous burden has been imposed on financial institutions of judging whether the nature of transaction raises suspicions. However, there is a risk of missing certain suspicious money laundering transactions because financial institutions may lack the capacity or expertise to analyse the suspicious funds or transactions.

In fact, the determination of suspicious transactions can be based upon the customer profile obtained through the CDD process. It means the obligation of reporting suspicious transactions can be a part of the extended requirement of CDD in some situations (Stessens, 2000, p. 162) The obligation of applying an enhanced CDD process in certain circumstances takes precedence over the obligation of reporting suspicious transactions.

5. The Impact of the preventive measures on financial privacy

The implementation of the preventive measures on financial service providers has raised controversial arguments about the risk of interference with financial privacy. Under the obligation of record keeping provided for in R11 of the 2012 FATF Recommendations (FATF, 2012), the identification data and transaction records should be available to domestic competent authorities upon appropriate authority. The reporting obligation may conflict with the desire for financial privacy. The interactions between the obligations to take preventive measures and bank secrecy (a notable form of financial privacy) will be addressed in detail below.

5.1 Concept and justifications for banking secrecy

Although banking secrecy appears to have a long historical development closely associated with the history of banking, modern banking secrecy actually evolved after World War I (Chambost, 1983, pp. 3-8). It was not legally recognized in the form of banking secrecy law until the 1930s. The first banking secrecy law was enacted in Switzerland in 1934, but since then it has flourished in many other States around the world (Chambost, 1983, pp. 5-6; Gagnon, 1990). Whilst the meaning of banking secrecy has been widely understood as the principle of confidentiality in financial transactions, there is no comprehensive concept or description of the term “banking secrecy” at the international level (Ping, 2004, p. 376). In general, banking

secrecy law protects a range of aspects of the relationship between bankers and their customer that are expressed in two main rules (Ping, 2004, p. 376): i) the banker shall not disclose the customer's financial information to interested parties, leaving aside a number of exceptions; and ii) the customer's financial information shall be protected legally from the intrusion of other parties.

Most States recognize and adopt some forms of banking secrecy based on a number of justifications (Chambost, 1983, pp. 91-259). The justifications vary from State to State, and thus, have resulted in a variety of legal bases for protecting banking secrecy at different levels of stringency. The justifications for banking secrecy derive from both the interest of the bank and its customers (Chambost, 1983, pp. 9-26). It should be recognized that although in certain States, banking secrecy is reinforced by statute and even protected by criminal sanction, it is not a part of universally accepted civil liberties or human rights (Moscarino, 1997, p. 177). According to English law, the banker-customer relationship is a contractual obligation, not an inalienable right (Ellinger *et al.*, 2006, pp. 117-21). Similarly, under German banking law, the foundation of the banker-customer relationship is dependent on a "general banking contract" (Mitsilegas, 2003, p. 127).

Most individuals want to prevent their financial information from being accessible by other interested parties. The demand for financial secrecy arises from the personal, business, political, fiscal or criminal motivations (Walter, 1990, pp. 1-4). In a cashless society, where most financial transactions are conducted through the banking system, banking records can directly reflect many aspects of a customer's affairs that he/she wants to keep secret. For instance, the financial records of a person can reflect his lifestyle, financial situation, or even every physical movement. Thus, organized criminals or political tyrants consider banking secrecy as a shield to hide and secure their assets. Money launderers rely on banking secrecy as a crucial tool facilitating their criminal activities. In addition, people possessing substantial wealth are often targets for criminals. Hence, these people often seek the skilled banking systems that provide strict banking secrecy. In response to the customer's demand for financial secrecy, divergent national and international bankers have offered banking secrecy as a kind of product. They compete with one another in terms of quality or cost of this type of product. Further, desirable banking systems are usually located in countries renowned for their political, social, economic and monetary stability.

This explains why some countries, e.g., Switzerland, Luxembourg or Hong Kong are known as "banking secrecy havens" (Chambost, 1983, pp. 145-250).

A number of countries have enacted strict banking secrecy laws with the aim of supporting their banking industries as well as their economies. Stringent banking secrecy has been used to attract foreign funds and to profit from the management of these funds (Moscarino, 1997, p. 184). Some of these countries are located in the Caribbean and South Atlantic close to unstable Latin American governments and drug producing countries. They include Antigua, the Bahamas, Bermuda, the Cayman Islands, Montserrat, the Netherlands Antilles, and Panama. Their geographical proximity and their stringent banking secrecy make them desirable destinations for capital flight and the proceeds of crime (Walter, 1990, pp. 210-21). In these countries, the banking secrecy law is an essential legal instrument of the banking industry which is a major contributor to their economies. However, these "banking secrecy havens" appear to make transnational money laundering more rampant and serious (Young, 2013, p. 161).

5.2 The instruments of banking secrecy

States choose different instruments to enforce banking secrecy. The most basic level of banking secrecy is achieved through a direct instrument, such as some type of deposit account: a "classic named account", "numbered account" or account under a false name (Chambost, 1983, pp. 39-67).

A "classic named account" allows withdrawal over the counter. A customer who wants to open this type of account normally has to provide his/her personal details, such as name, address, and a sample signature for the bank. The sample signature allows the cashier to recognize the customer when withdrawing cash over the counter.

A "numbered account" or account held under a false name is an account where the holder is denoted for general purposes by a number or code, or sometimes a pseudonym. The identity and other personal details of the customer are known only to a limited number of bank staff members who are responsible for the relationship with the customer. Others, who process the transactions for the bank account, only know the number, code or pseudonym. A "numbered account" is a well-known direct instrument of banking secrecy protecting the customers from unauthorised disclosure. It was an essential banking secrecy instrument in the Swiss banking system from the 1950s (Chaikin, 2005, pp. 101-02). Nonetheless, under pressure from the international

community, in 2003 Switzerland introduced its new Money Laundering Law which forces Swiss banks to reveal the name of customers when transferring money abroad. Though the numbered account has not disappeared entirely, customers are no longer able to hide their identity when making transactions abroad.

The indirect instruments of banking secrecy include "shell companies" or "offshore captive banks" (Chambost, 1983, pp. 58-75). "Shell companies" or anonymous corporations are non-publicly traded corporations, limited liability companies and other business entities (e.g., trusts) that have no physical presence other than a mailing address and generate little or no independent economic value. A financial institution may provide financial services for these entities, such as internet banking or currency exchange (Sharman, 2010, pp. 130-32). "Shell companies" may serve legitimate commercial purposes, such as: holding stock or intangible business assets, facilitating domestic and cross-border currency and asset transfers, and facilitating corporate mergers (Floros and Sapp, 2011, pp. 851-52). These companies are easy and inexpensive to set up and operate; beneficial ownership is securely anonymous, and transaction details can be concealed from regulatory and law enforcement agencies. Thus, this kind of company has been seen as a big business, and States compete at offering more secure anonymity along with other benefits in incorporation services. In the US, the United Kingdom (UK) and other States with lax incorporation requirements, "shell companies" are freely available to anyone with an internet connection and some money (Sharman, 2010, pp. 130-32). However, "shell companies" can aid criminals by providing the appearance of legitimacy and access to the national and international financial system through their bank accounts. "Shell companies" may be formed and then open corporate bank accounts for illegal purposes. The transactions processed through the corporate accounts of such a "shell company" are effectively untraceable and are thus very useful for the purpose of concealing criminal proceeds (Sharman, 2010, pp. 127-30). The US has recently paid more attention to the problems of "shell companies" as part of their on-going AML and combating terrorist financing initiatives. Financial Crimes Enforcement Network (FinCEN) of the US, stated that "lack of transparency in the formation and operation of shell companies may be a desired characteristic for certain legitimate business activity, but it is also a vulnerability that allows these companies to disguise their ownership and purpose" (FinCEN, 2006, p. 1). Furthermore, the problems of "shell companies" have been widely identified in various reports and research projects on combating some transnational crimes, such as: drug trafficking-related

crimes, terrorism, money laundering, corruption, or tax evasion (Sharman, 2010, p. 129). As a result, a number of international legal instruments have obliged financial institutions that the beneficial ownership of legal persons and legal arrangement must be ascertained (R10, 22, 24 and 25 of the 2012 FATF Recommendations).

Another indirect instrument of banking secrecy is "captive bank", which is a bank that exists purely for the benefit of one natural or legal person or a group of people (Walter, 1990, pp. 43-44). Traditionally, it is the wholly of partially owned subsidiary of a company. For example, A, B and C are companies that belong to Mr X who also controls captive bank D. Bank D is established primarily to fulfil the financial requirements of Mr X's companies. It generally offers all basic banking services (e.g., safe-keeping of deposits). In some cases, it may provide additional services, for example merchant banking. To maximize profits, captive banks are usually offshore banks located in "tax havens". An offshore "captive bank", which is resident in a "tax haven", may enjoy various benefits (Walter, 1990, pp. 43-44), such as lax tax liability and greater privacy resulting from the stringent banking secrecy laws in the country of location. This kind of bank obviously provides a useful tool for money launderers.

5.3 Preventive measures challenging banking secrecy

Because banking secrecy has been exploited as an effective tool to secure the proceeds of crime, in most jurisdictions there are certain compulsory circumstances in which banking secrecy is lifted or relaxed to serve the fight against crime. The information disclosed by the banks and used by competent authorities is very important in protecting the bankers as well as in AML. Lifting banking secrecy under certain circumstances has also been embodied in a number of international legal instruments with the aim of cooperating in the fight against transnational crime (e.g., article 5(3) of the United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (UN, 1988); and R10 of the 2012 FATF Recommendations).

Under the international AML regime, national banking systems cultivating a tradition of stringent banking secrecy now have to harmonize with the new international standard of banking secrecy. The preventive measures, especially the reporting obligation, raise controversial questions whether there are conflicts between this obligation and the demand of banking secrecy, and whether this obligation has negative effects on the commercial interests of bankers (Ping,

2004, p. 380). The answers to these questions will depend on what the reported information is about, who it concerns, and what it will be used for.

It is noteworthy that the objectives of the preventive measures taken by banks not only serve the AML initiatives but also protect the banks from reputational damage, loss of public confidence or other damages resulting from being used for criminal purposes. Thus, banks should implement the preventive measures in compliance with international standards in order to protect themselves from the harms of money laundering. Further, the adequate implementation of the preventive measures has been seen as a market tool to guarantee the stability and health of banks in the global financial market (Verhage, 2008, p. 10).

However, bankers should not have to lift banking secrecy in unreasonable situations. For example, the lack of the appropriate standards of suspicious transactions may result in unreasonable reports being made to law enforcement agencies. These reports may affect the interests of the banker and its customers because of the financial information disclosed. The extent to which banking secrecy is relaxed depends on the balance between the interests of law enforcement and bankers. For instance, absolute banking secrecy should not exist when there is a criminal threat to the banking system; or when the higher interest of the public or State such as in case of fighting against crime is involved. Nevertheless, in practice, it is difficult to find the right balance between the two potentially competing interests (Ping, 2004, p. 380).

6. Conclusion

In brief, ensuring the adequate implementation of the preventive measures is highly important for financial institutions to be secure from money laundering. Nonetheless, the enforcement of these measures is becoming much more intrusive into financial privacy which are themselves strongly justified by legitimate and undisputed rationales. This leads to tension and potential conflicts of interests between law enforcement authorities and financial service providers, between the protection of privacy rights and the objectives of the preventive measures. In practice, financial privacy should be weighted fairly against the objectives of preventive measures in AML. In addition, financial institutions should be equipped with sufficient means and capacity for effective customer identification to prevent the risk of becoming involved unknowingly in money laundering.

References

Basel Committee on Banking Supervision (1988), "Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering ", available at: http://www.bis.org/publ/bcbsc137.pdf (accessed 20 January 2017).

Basel Committee on Banking Supervision (2001), "Customer Due Diligence for Banks", available at: http://www.bis.org/publ/bcbs85.pdf (accessed 21 January 2017).

Chaikin, D. (2005), "Policy and Fiscal Effect of Swiss Bank Secrecy", *Revenue Law Journal,* Vol. 15, No. 1, p. 21.

Chambost, E. (1983), *Bank Accounts: A World Guide to Confidentiality* John Wiley & Sons.

Ellinger, E.P., Lomnicka, E. and Hooley, R. (2006), *Ellinger's Modern banking law* 4th edn, Oxford University Press.

FATF (1990), "The Forty Recommendations of the FATF", available at: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%201990.pdf (accessed 24 January 2017).

FATF (2012), "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - the FATF Recommendations", available at: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf (accessed 3 January 2017).

FinCEN (2006), "Potential Money Laundering Risks Related to Shell Companies ", available at: http://www.fincen.gov/statutes_regs/guidance/pdf/AdvisoryOnShells_FINAL.pdf (accessed 20 January 2017).

Floros, I.V. and Sapp, T.R.A. (2011), "Shell games: On the value of shell companies", *Journal of Corporate Finance,* Vol. 17, No. 4.

Gagnon, R. (1990), "International Banking Secrecy: Developments in Europe Prompt New Approaches", *Vanderbilt Journal of Transnational Law,* Vol. 23.

Grant, T.D. (1995), "Toward a Swiss Solution for an American Problem: An Alternative Approach for Banks in the War on Drugs", *Annual Review of Banking Law* No. 14.

IAIS (2003), "Insurance Core Principle and Methodology ", available at: http://www.iaisweb.org/__temp/Insurance_core_principles_and_methodology.pdf (accessed 22 January 2017).

IAIS (2004), "Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism", available at: http://www.iaisweb.org/__temp/Guidance_paper_on_anti_money_laundering_and_combating_the_financing_of_terrorism.pdf (accessed 25 January 2017).

IOSCO (2004), "Principles on Client Identification and Beneficial Ownership for the Securities Industry ", available at: http://www.cnmv.es/publicaciones/IOSCO_seguridad.pdf (accessed 25 January 2017).

Koker, L.d. (2006), "Money Laundering Control and Suppression of Financing of Terrorism: Some Thoughts on the Impact of Customer Due Diligence Measures on Financial Exclusion", *Journal of Financial Crime* Vol. 13, No. 1.

Mitsilegas, V. (2003), *Money Laundering Counter-Measures in the European Union: A New Paradigm of Security Governance Versus Fundamental Legal Principles* Kluwer Law International.

Moscarino, G.J. (1997), "Beating the Shell Game: Bank Secrecy Laws and Their Impact on Civil Recovery in International Fraud Actions", *Company Lawyer,* Vol. 18, No. 6.

Mulligan, D. (1998), "Know Your Customer Regulations and the International Banking System: Towards a General Self-Regulatory Regime", *Fordham international law journal,* Vol. 22.

Picot, G. (2002), *Handbook of International Mergers and Acquisitions: Preparation, Implementation, and Integration*, Palgrave Macmillan.

Ping, H. (2004), "Banking Secrecy and Money Laundering", *Journal of Money Laundering Control* Vol. 7, No. 4.

Sharman, J.C. (2010), "Shopping for Anonymous Shell Companies: An Audit Study of Anonymity and Crime in the International Financial System", *Journal of Economic Perspectives,* Vol. 24, No. 4.

Stessens, G. (2000), *Money Laundering: A New International Law Enforcement Model*, Cambridge University Press, Cambridge.

Thony, J.F. (1996), "Processing Financial Information in Money Laundering Matters: The Financial Intelligence Units", *European Journal of Crime, Criminal Law and Criminal Justice,* Vol. 4.

UN (1988), "United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances" *1582 UNTS 95, 20 December 1988*, entered into force 11 November 1990.

UN (2000a), "Interpretative Notes for the Official Records *(travaux préparatoires)* of the Negotiation of the United Nations Convention against Transnational Organized Crime and the Protocols thereto" *A/55/383/Add.1*, 3 November 2000.

UN (2000b), "United Nations Convention against Transnational Organised Crime" *2225 UNTS 209, 15 November 2000*, entered into force 29 September 2003.

UN (2003), "United Nations Convention against Corruption" *2349 UNTS 41, 31 October 2003*, entered into force 14 December 2005.

UNODC (2004), "Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime and the Protocols thereto", available at: http://www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf (accessed 21 June 2016).

Verhage, A. (2008), "Between the Hammer and the Anvil? The Anti-Money Laundering Complex and its Interraction with the Compliance Industry", *Crime, Law and Social Change* Vol. 52, No. 1, p. 24.

Walter, I. (1990), *The Secret Money Market : Inside the Dark World of Tax Evasion, Financial Fraud, Insider Trading, Money Laundering, and Capital Flight*, Harper & Row Ballinger Division, New York.

Wolfsberg Group (2012), "Wolfsberg Anti-Money Laundering Principles for Private Banking ", available at: http://www.wolfsberg-principles.com/pdf/Wolfsberg-Private-Banking-Prinicples-May-2012.pdf (accessed 21 January 2017).

Young, M.A. (2013), *Banking Secrecy and Offshore Financial Centers: Money Laundering and Offshore Banking*, Routledge.

Corresponding author

Dr Chat Nguyen Le can be contacted at: chat.nguyen@fnu.ac.fj