The FATF's customer identification framework: fit for purpose?

Louis de Koker

(School of Law, Deakin University, Melbourne, Australia)

Abstract:

Purpose

– This paper aims to investigate the purpose, reach and effectiveness of the customer identification framework of the Financial Action Task Force (FATF).

Design/methodology/approach

– The article draws on relevant research and documents of the FATF, the Basel Committee on Banking Supervision and the Alliance for Financial Inclusion to determine whether compliance with the standards and practices of the FATF would prevent anonymous usage of financial services.

Findings

– The FATF's identification principles, guidance and practices resulted in processes that are largely bureaucratic and do not ensure that identity fraud is effectively prevented. Strict identification requirements on the other hand may impact on financial inclusion, leaving the FATF with little leeway to raise its standards. There are potential solutions, but they are longer-term and partial in nature.

Originality/value

– Current identification and verification practices affect the lives of millions of people around the globe. The measures are being enforced to ensure that users are appropriately identified. This article informs the debate by highlighting the weaknesses of the current approach.

The Financial Action Task Force (FATF) sets international standards to be met by countries, financial institutions and designated non-financial businesses and professions to combat money laundering and terrorist financing. To this end, specific FATF Recommendations set customer identification requirements to prevent anonymous business relationships, especially anonymous bank accounts. These anti-money laundering (AML) and counter terrorist financing (CTF) standards are aimed at increasing transparency of financial services. Banks that comply with these standards may, however, not necessarily ensure identification of customers. The article considers the current principles and limits of the current regime and whether the approach can be improved.

The FATF Recommendations extend to a large number of financial and also non-financial institutions, but for the sake of simplicity, this paper is restricted to the duties of banks. The focus is furthermore limited to individual customers that interact in their own capacity with banks. Beneficial owners and corporate identification give rise to additional layers of complexity that lie beyond the scope of a single article.

A brief overview of the current identification standards of the FATF is provided before the focus of this article shifts to the meaning of “identification” and “verification” within the FATF framework.

FATF: customer due diligence and record-keeping

The FATF’s Recommendation 10 (Financial Action Task Force, 2012), read with its Interpretative Note, sets out the requirements regarding customer identification and verification. It commences by stating that countries should prohibit financial institutions from keeping anonymous accounts or accounts in obviously fictitious names and proceeds to state that these institutions should be required to undertake customer due diligence (CDD) measures when:

◦ establishing business relations;

◦ carrying out occasional transactions: above the applicable designated threshold (USD/EUR 15,000), or that are wire transfers in the circumstances covered by the Interpretive Note to Recommendation 16;

◦ there is a suspicion of money laundering or terrorist financing; or

◦ the institution has doubts about the veracity or adequacy of previously obtained customer identification data.

The following CDD measures must be taken:

◦Identifying the customer and verifying that customer’s identity using reliable, independent source documents, data or information.

◦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.

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

◦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.

It is important to note that compliance with the CDD standards of Recommendation 10 (excluding the ban on anonymous accounts) should be implemented on a risk-based approach. In terms of this approach, that now underpins compliance with the FATF standards, countries and institutions are required to assess their money laundering and terrorist financing risks and to adopt appropriate,

proportional compliance responses. Where higher risk is identified, enhanced CDD measures must be adopted. In the case of lower risks, countries may allow their banks to adopt simplified measures. Where there is proven low risk, regulators may also consider exempting relevant institutions, products and services from AML/CTF obligations.

Standard, enhanced and simplified CDD

Enhanced and simplified CDD measures imply that there is a standard level of CDD that applies to customers, products or services that pose a medium or standard level of risk. The FATF does not stipulate what standard CDD measures should entail. In its guidance document on financial inclusion, the FATF commented as follows (Financial Action Task Force, 2013a, par. 67):

> ***The FATF Recommendations do not specify the exact customer information (referred to by certain countries as 'identifiers') that businesses subject to AML/CTF obligations should collect to carry out the identification process properly, for standard business relationships and for occasional transactions above USD/EUR 15,000. Domestic legislation varies, although common customer information tends to consist of name, date of birth, address and an identification number. Other types of information (such as the customer's occupation, income, telephone and e-mail address, etc.) are generally more business and/or anti-fraud driven and do not constitute core CDD information that must be collected as part of standard CDD-although such information could appropriately be part of enhanced CDD for higher risk situations.***

In addition to collecting the standard as well as supplementary information about a customer, enhanced CDD may also involve stricter verification processes and closer monitoring of transactions. The precise measures to be taken will depend on the risks that must be mitigated.

Where risks are lower, institutions may be allowed to adopt simplified CDD measures. These measures should be commensurate with the lower-risk factors and may relate to all or only to some of the CDD measures, depending on what is required to mitigate the relevant risks. Without limiting the nature of the simplified measures, the FATF listed the following examples (Financial Action Task Force, 2012, INR 10 par 21):

◦ verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if account transactions rise above a defined monetary threshold);

◦ reducing the frequency of customer identification updates;

◦ reducing the degree of ongoing monitoring and scrutinizing of transactions, based on a reasonable monetary threshold; and

◦ not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established.

Simplified CDD measures are, however, not acceptable whenever there is a suspicion of money laundering or terrorist financing, or where specific higher-risk scenarios apply (Financial Action Task

Force, 2012, INR 10 par 21). These scenarios include doing business with foreign politically exposed persons (PEPs), who should be subjected to enhanced CDD, as they are considered as posing higher risks per se (Financial Action Task Force, 2012, Rec 12). Wire transfers are also excluded from the ambit of general risk-based measures (Financial Action Task Force, 2012, Rec 16). Specific rules apply to wire transfers and in terms of those rules, some simplification may be allowed in relation to low-value cross-border wire transfers: Countries may adopt a de minimis threshold value for cross-border transfers (no higher than USD/EUR 1,000) below which the identities of the parties do not need to be verified and limited information may be permitted to accompany such transfers (Financial Action Task Force, INR 16 par 5).

Identification and verification

The FATF Recommendations do not define "identify" or "identification" for CDD purposes.

According to the Oxford Dictionary (Oxford Dictionaries, 2013), the verb "identify" carries the following two meanings:

1. to establish or indicate who or what (someone or something) is; and

2. to associate someone or something closely with someone or something.

The noun "identification" means:

◦ the action or process of identifying someone or something or the fact of being identified;

◦ a person's sense of identity with someone or something; or

◦ the association or linking of one thing with another.

The non-mathematical meaning of the noun "identity" means:

◦ the fact of being who or what a person or thing is; or

◦ a close similarity or affinity.

While "identify" carries a range of meanings, it is submitted that in the FATF context, it means establishing a prospective or current customer's unique identity.

The FATF standards are not only concerned with the recording of identifying particulars but also with "verification". Verification refers to the authentication of the identifying particulars (Financial Action Task Force, 2013a, par. 66). The bank is expected to refer to reliable, independent source documents, data or information to verify the customer's identifying particulars. Identification and verification are inter-related but separate processes (Chatain et al., 2011, p. 77). Identification is completed when sufficient information is obtained to enable the institution to establish who the customer is.

Verification processes, on the other hand, are undertaken to obtain assurance that some or all of the obtained information is actually correct and relates to that particular customer.

While the FATF's Recommendations advise institutions not to keep anonymous accounts or accounts in obviously fictitious names, they do not specifically clarify their concept of anonymity. In discussions with various FATF representatives and stakeholders, they generally used "anonymous" and "not correctly identified" synonymously. They tended to classify a customer as anonymous or as not identified for FATF purposes in cases such as the following:

◦ where no customer particulars are collected to enable the bank to establish who the customer is;

◦ where too little information is collected about a customer to enable the bank to establish who the customer is (this includes the case where comprehensive information is gathered and verified regarding another person, for instance a puppet who is clearly controlled by or acting for the benefit of the beneficiary, and no steps are taken to identify, verify and record the particulars of the beneficiary);

◦ where reasonable steps are not taken to verify a person's identifying particulars (this may overlap with the prohibition against opening an account in an obviously fictitious name where the customer's actual identity is not recorded);

◦ where information is collected and verified but not correctly recorded and retained to ensure that the bank retains its knowledge about the customer's identity; and

◦ where information is collected and verified but identifying particulars are not updated and refreshed with the result that the bank after some time is unable to state with confidence that it knows who the customer is.

The FATF's concept of identification appears focused on processes and documents rather than substance: A customer has not been correctly identified if the bank failed to collect prescribed identifying particulars of that customer or failed to verify the person's identity. The fact that the banker personally knows the customer well is of little relevance if the prescribed details were not collected, verified and recorded in terms of the bank's policies and the applicable statutory obligations of the bank.

The purpose of identification and verification measures

The FATF has not explicitly stated the purpose of identification and verification processes. It is generally deemed obvious that they are aimed at ensuring that banks know business and signification transactional customers.

Does that mean that the measures are aimed at preventing identity fraud? FATF is certainly concerned about identity fraud and theft, especially relating to new payment methods (Financial Action Task Force, 2010, par 42; Financial Action Task Force, 2013b). FATF's approach to customer identification, however, leaves a question mark as to whether the prevention of identity fraud is a distinct objective of these standards. Whether the AML/CTF identification and verification measures can effectively assist in preventing identity fraud depends largely on their stringency and integrity of the processes. The stringency in turn depends on factors such as the information collected on a

customer and the quality of that information. The quality of the information gathered is closely linked to verification processes. FATF's approach to these aspects and the weaknesses that the approach introduced will be explored in greater detail below.

What information should generally be collected about a customer?

Before the adoption of the 2003 standards and the "Customer Due Diligence" language, the term "Know Your Customer" (KYC) was often used. KYC and CDD are broader than mere identification and verification of identities and are closely linked to the concept of customer profiling.

The FATF's CDD principles refer to profiling of customers and the need to monitor the customer's activity to ensure that the transactions being conducted are consistent with the bank's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds. The Basel Committee on Banking Supervision (BCBS) views profiling as central to CDD and customer risk mitigation. From the BCBS perspective, the identification and verification processes are therefore not merely aimed at recording the customer's correct name but at obtaining sufficient information to draw an appropriate business and risk profile of the customer (Basel Committee on Banking Supervision, 2001, pp. 3-4). Profiling enables the bank to assess and mitigate the risks posed by the customer. It also supports customer monitoring because it assists the bank to anticipate the customer's normal transaction pattern. A transaction that deviates from that pattern may attract the attention of the bank's customer monitoring program and may result in a report to the Financial Intelligence Unit. The reliability of profiling depends however on the sufficiency and accuracy of the customer information that is gathered.

According to the BCBS, the following information should be obtained from a customer for purposes of standard CDD (Basel Committee on Banking Supervision, 2003, par. 10):

For natural persons, the following information should be obtained, where applicable:

◦ legal name and any other names used (such as maiden name);

◦ correct permanent address (the full address should be obtained; a Post Office box number is not sufficient);

◦ telephone number, fax number and e-mail address;

◦ date and place of birth;

◦ nationality;

◦ occupation, public position held and/or name of employer;

◦ an official personal identification number or other unique identifier contained in an unexpired official document (e.g. passport, identification card, residence permit, social security records, driving license) that bears a photograph of the customer;

◦ type of account and nature of the banking relationship; and

◦ signature.

The bank should use that information to draw and assess a customer's risk profile. Where customers are assessed as having a higher risk profile, additional inquiries must be made or information obtained, for example relating to the person's address, source of wealth or prior banking relationships (Basel Committee on Banking Supervision, 2003).

The BCBS guidance has shaped current banking practices and supervisory expectations. In 2012, the Alliance for Financial Inclusion surveyed the customer identification practices of a group of developing country members. The survey reflects the extent to which the extensive list of the BCBS impacted on identification practices relating to customers with a standard risk profile (Alliance for Financial Inclusion, 2013; Table I).

While this overview of customer information requirements in the six countries reflects extensive collection of information by some, it is also noticeable that this pattern is not consistent. South Africa, a FATF member since 2004, for example, only requires the bare minimum to be collected.

The BCBS guidance is currently being revised to reflect the 2012 revised Basel Core Principles for Effective Banking Supervision as well as the 2012 revised FATF Recommendations. The general thrust of the BCBS approach remains, although the list of identification particulars and verification options does not appear in their 2013 discussion document. The discussion document does however still emphasize profiling as an important first step in risk-rating customers (Basel Committee on Banking Supervision, 2013).

Differences between the FATF and BCBS views of profiling

There is evidence of differences between the post-2012 BCBS and FATF views of profiling. The 2013 FATF guidance on financial inclusion discusses the minimum particulars that banks should obtain from customers. According to the FATF, information such as the customer's occupation, income and contact details does not constitute core CDD information that must be collected as part of standard CDD (Financial Action Task Force, 2013a, parr. 75 and 102). This is not the view held by the BCBS (Basel Committee on Banking Supervision, 2013, par 30). It is submitted that it is unlikely that a reliable customer profile for AML/CTF purposes can be drawn without information about a customer's occupation and income (De Koker, 2011, pp. 376-377).

FATF's simplified CDD processes also fit uncomfortably with the BCBS profiling approach. In terms of the BCBS approach, sufficient information must be collected to draw an appropriate risk profile and, where the customer is assessed as posing a higher risk, additional steps should be taken. The FATF model allows for upfront, mainly product-based profiling and for very limited information to be gathered where the risks are assessed as lower. In this context, the FATF acknowledged that there is a risk that monitoring of transactional activity may fail in the context of simplified CDD. This would happen when too little information is gathered to profile a customer, thereby undermining the ability of monitoring mechanisms to identity suspicious and unusual activity (Financial Action Task Force, 2013a, par 76). Although the FATF noted this possibility, it has not provided further guidance on how this result can be avoided.

The general impression is therefore that the FATF, unlike the BCBS, does not regard profiling and the extensive collection of identifying particulars and contextual customer information as central to general CDD. It does recognize its value in relation to higher-risk customers, but its approach indicates that this view does not extend to lower-risk customers or even standard-risk customers.

Where limited information is gathered about a customer, the ability of identification and verification measures to combat identity fraud depends very heavily on the identifying value of the information and on its verification. The limitations of the FATF approach in respect of verification will be discussed below.

In conclusion it should be noted that FATF and the BCBS differences appear to extend beyond profiling to the level and stringency of CDD in general. While the FATF in 2012 adopted a risk-based approach that allows for simplified CDD in lower-risk cases, the BCBS in the same year adopted a strict approach to CDD when it issued its revised Core Principles for Effective Banking Supervision in 2012 (Basel Committee on Banking Supervision, 2012). Core Principle 29 (Abuse of financial services) states that “the supervisor should determine that banks have adequate policies and processes, including strict customer due diligence (CDD) rules to promote high ethical and professional standards”. It is not clear that the concept of “strict” CDD rules as envisaged by the BSBS would include adopting simplified CDD in lower-risk cases.

Stringency of the verification measures

A bank meets key AML/CTF obligations if it gathers prescribed identifying information about a prospective customer and ensures that prescribed steps are taken to verify the customer’s particulars. As pointed out above, the FATF requires the person’s identity to be verified “using reliable, independent source documents, data or information”. The FATF has not given specific guidance regarding to the source documents, data or information that it regards as reliable or regarding its test for reliability. This is a matter that it generally leaves to countries to determine (Financial Action Task Force, 2013a, par 77). In general however, the FATF endorsed processes that require information to be verified against formal government-issued documentation such as a national identity document, Medicare card, driver's license, etc. The assumption is that these documents offer reliable proof of information set out in it.

The reliability of such state-issued documentation differs from country to country. Although reliability is vital to the efficacy of the verification processes, FATF has not addressed it comprehensively. While the FATF obviously prefers the use of reliable state-issued documentation, neither its pre-2013 mutual evaluation procedures nor those for the fourth round of mutual evaluations (Financial Action Task Force, 2013c) explicitly require assessors to investigate and comment on the reliability of state-issued documents of countries. The mutual evaluation reports produced in the third round of mutual evaluations do not provide a comprehensive or even consistent picture in this regard. In general, the evaluation methodology supports a box-ticking approach: If a country compels its institutions to verify identities using state-issued documents, it would generally be rated as technically compliant with the verification standard, even though the reliability of those documents may be questionable. Whether reliability will be considered in the fourth round of mutual evaluations as part of an assessment of effectiveness, will be in the hands of individual assessment teams.

Financial Action Task Force's 2009 mutual evaluation report provides a good example of the general FATF assessment approach in this regard. The report records that regulated institutions are required to identify and verify the identities of their customers using official South African identification documents (Financial Action Task Force, 2009, par 398). Yet, no remark was made about the serious concerns regarding the integrity of the official South African identity document and passport (SAPA, 2005). For some years, there was growing national and international concern regarding the integrity of the documents. Corrupt officials of the South African Department of Home Affairs, the government department that issues passports and identity documents, have issued original documents in the names of choice to undocumented migrants, refugees and criminals. In February 2009, it was announced that the United Kingdom was imposing visa restrictions from March 2009 on the more than 400,000 South Africans who visit the UK each year, because genuine South African passports can be bought too easily from corrupt officials. Although the South African government has repeatedly acknowledged the problems and embarked pre-2009 on actions to improve the integrity of the national identification infrastructure, the 2009 FATF report was silent on the matter.

Verification challenges are however not confined to countries with unreliable national identification systems. Even in countries where the documentation is reliable, very few institutions train their employees to identify forged documents. The verification processes may therefore fail to provide reasonable assurance. Most crucially, these failures are more likely in the case of criminals and terrorists who wish to hide or disguise their identities by obtaining high-quality false verification documentation. It is ironic that the failure of the verification procedure is therefore more likely to occur in the very cases that the system attempts to prevent.

The limits of the FATF identification principles

The FATF's lack of clarity regarding the particulars required for identification purposes, its apparent rejection of the more extensive profiling requirements of the BCBS and its lack of consistent assessment and enforcement of usage of reliable verification documents, data and information, undermine the general identity fraud combating value of its identification and verification measures.

The FATF's risk-based approach and exemptions as well as the development of new payment methods may limit the value of these measures further.

The risk-based approach to CDD

To shift AML/CFT resources to higher-risk scenarios and to facilitate financial inclusion, FATF allows for the adoption of simplified CDD measures in relation to lower-risk customers, products and services. In practical terms, simplified measures may allow for less customer information to be gathered and less stringent verification of that information. In the financial inclusion space, money laundering and terrorist financing risk are often mitigated by a range of restrictions that ensure that the relevant products involve low-value amounts (Isern and de Koker, 2009). Although these restrictions may mitigate money laundering risk and arguably also terrorist financing risk, the simplified identification and verification measures are not necessarily effective to combat identity fraud in relation to those products.

FATF exemptions

The footprint of the FATF standards does not extend to all financial transactions. National laws, for example, may allow a bank to conclude a non-account-based transaction of USD 14,000 without asking for identification and verification of the customer. This is possible as occasional transactions involving less than USD/EUR 15,000 are not covered by the FATF scheme. Countries may furthermore adopt a de minimis threshold value for cross-border transfers (no higher than USD/EUR 1,000) below which the identities of the parties do not need to be verified and limited information may be allowed to accompany such transfers (Financial Action Task Force, 2012, INR 16 par 5).

The 2012 Recommendations also opened to the door to another intriguing possibility. They recognize that CDD can be simplified in lower-risk cases by, among others, “verifying the identity of the customer and the beneficial owner after the establishment of the business relationship (e.g. if account transactions rise above a defined monetary threshold)” (Financial Action Task Force, 2012, INR 10 par 21). A customer holding an account where the balance or the value of the transactions does not rise above the defined threshold will therefore remain unverified. This outcome would run counter to the FATF’s general ban on anonymous accounts but is allowed as an exception. This exception is of course only allowed where the bank does not suspect the customer of money laundering or terrorist financing.

Mexico has taken the concept of anonymity in low-risk financial services one step further. They implemented a tiered risk-based approach to bank accounts where the risk control measures increase in relation to the functionality of the accounts. The most basic account is not subject to any customer identification and verification requirements. The Mexican tiered approach is based on a mixture of low-risk exemptions from FATF controls and simplified CDD measures in relation to lower-risk products.

The anonymous Mexican accounts are subject to various restrictions to limit risks of money laundering or terrorist financing abuse (Alliance for Financial Inclusion, 2013). Monthly deposits are, for example, restricted to 750.00 UDIS (around USD $250) with a non-cumulative balance limit of 1,000 UDIS (around USD $350). Accounts may only be held by natural persons, cannot be linked to a mobile money account and must be opened in person. The accounts can furthermore only be used for domestic transactions and cannot be used to transfer amounts to other accounts or financial products. They may be used to receive remittance payments, but in that case, the names of the originator and the

beneficiary must be recorded. The accounts are monitored and suspicious transactions must be reported to the Financial Intelligence Unit.

The FATF Recommendations prohibit anonymous accounts and the Mexican model appears to be in breach of this prohibition. The FATF standards, however, also allow countries not to apply some of the Recommendations provided that there is a proven low risk of money laundering and terrorist financing, that this occurs in strictly limited and justified circumstances and that it relates to a particular type of financial institution or activity (Financial Action Task Force, 2012, INR 1 par 6). Mexico argues that the usage restrictions and controls imposed on these basic accounts bring these anonymous accounts within this exemption. Whether this approach meets the FATF standards will be assessed during the Fourth Round of Mutual Evaluations and the answer may depend heavily on the quality of the risk assessment that informed the Mexican model. If the FATF approves the scheme, a number of other countries are set to follow their example and create categories of anonymous, low-risk accounts.

New payment methods

The FATF is very concerned about the money laundering and terrorist financing risks posed by new payment methods such as mobile money (Chatain et al., 2011), Internet banking, cyber currencies and prepaid cards (Financial Action Task Force, 2013b). New payment methods do pose risks of anonymous usage, depending on the design of the applicable regulations and the applicable business model. However, the FATF's work on new payment methods does not sufficiently address the risks of anonymous usage that is linked to older technology such as automatic teller machines, debit cards and credit cards. These allow for services to be secured by one, identified person but used by other, unknown and unidentified parties. Similar potential lies in individual beneficial ownership structures and corporate structures, which fall outside the scope of this article.

Some solutions

The FATF finds itself in a bind. AML/CTF measures, especially CDD measures, are expensive (Sathye, 2008; Veris Consulting, 2013). They also exact a social cost, as the verification requirements may form barriers that prevent socially marginalized people from accessing financial services (De Koker, 2006; Bester et al., 2008).

An obvious solution to the lack of effectiveness of the current measures is to require more robust identification and verification practices in respect of not only higher-risk services but also lower-risk services. That would however increase the costs of the current processes and undermine financial inclusion. Where AML/CTF measures undermine financial inclusion, overall ML/FT risk may increase, as significant numbers of persons will have to continue to use non-transparent, cash-based and informal financial services (Financial Action Task Force, 2013a, parr. 1-3). Such measures may therefore increase the integrity risks that the FATF attempts to mitigate.

The current FATF measures are of course perversely also one of the factors driving identity fraud on banks: If banks did not have identification processes to combat money laundering and terrorist financing, criminals would not have to resort to using false identities to open and operate accounts.

Increasing identification requirements to combat identity fraud may therefore also generate additional identity fraud.

Improve national identification systems

A partial but longer-term solution lies in improving the reach and the integrity of national identification systems (Isern and de Koker, 2009). Nigeria and India are examples of countries that are in the process of providing national identity numbers and national identity cards to millions of citizens and residents (Dass, 2011; Gold, 2011; Gelb and Clark, 2013). Although the relevance of improved national identification infrastructure to AML/CFT was noted before 2012 (Bester et al., 2008), the FATF did not address this in its revised standards. Of course, even if full coverage is reached, it will not address the identification issues that currently plague countries with unreliable national identification systems.

Identifiability

The current FATF approach attempts to ensure that all customers are identified. Despite the costs of the measures and their negative impact as a barrier to financial services, these processes are not necessarily sufficiently robust to ensure that customers are actually identified.

New payment methods, especially mobile money, provide the ability to identify and locate an unidentified user. This potential developed since the FATF standards took form in the late 1980s. Mobile phone usage reveals much about the behavioral patterns, personal preferences and social networks of customers. The data are even richer where the customer also uses the mobile phone for financial transactions. When combined and mined with sophisticated data-mining tools, unidentified users may be identified (De Montjoye et al., 2013).

Such data collection and mining by financial and the telecommunications service providers present significant risks of abuse not only by the private sector and criminals but also by authorities (Paik, 2010; Jentzsch, 2012; Harris et al., 2013; De Koker and Jentzsch, 2013). There are therefore sound reasons to ensure that appropriate legal and other controls apply. In the context of AML/CTF however, this capability may provide an alternative to the current large-scale identification approach. It enables the identification of the few when required by law enforcement, rather than the comprehensive but unsuccessful attempt to identify all users, just in case law enforcement may be interested in some.

Profiling

Profiling in the AML/CFT space, as discussed earlier, means the collection of sufficient data about the customer to enable a bank to assess the risks posed by that customer and to anticipate the general pattern of conduct of the customer. It is possible to use profiling to manage money laundering and terrorist financing risks even when verification does not occur. Profiling is, for example, gaining traction in the credit scoring space where Big Data analytics are used to determine the likelihood of repayment of a small loan by a person who does not have a credit record (Kumar and Muhota, 2012; Lobosco, 2013). In the AML/CTF context, it may allow for a model where a customer for a lower-risk product is identified and has to provide profiling information, but where verification is not undertaken

upfront. Where such customers' usage of the product diverges from the expected pattern, they may be refused further services or may have their transactions suspended until they enable the bank to verify their identifying particulars. Identification and profiling can therefore provide increased risk mitigation benefits in relation to lower-risk products, without posing the financial inclusion barriers that are inherent in many verification practices (Isern and de Koker, 2009).

Conclusion

The FATF's identification and verification framework was developed to ensure that banks know who their customers are. There is however little evidence that the current FATF approach is designed to achieve that purpose effectively. The FATF has been vague on identification practices and appear to disagree with the BCBS's approach regarding profiling. Neither has it instructed its assessors to consistently consider and assess the adequacy of the verification measures that are undertaken. While enhanced due diligence measures generally offer a higher level of comfort and certainty, the measures in relation to standard-risk and lower-risk customers are not necessarily sufficiently robust to prevent identity fraud. As a result, the current AML/CTF identification and verification processes are often expensive box-ticking exercises that inconvenience the honest but do not effectively bar the dishonest from using false identities to access financial services.

This approach is not set to change under the new, mandatory risk-based approach of the FATF. Under this approach, regulators and banks will have more leeway to determine appropriate identification and verification measures for customers with different risk profiles. Identification and verification measures are set to be relaxed in relation to products and services that are assessed as posing a lower money laundering and terrorist financing risk. This is vital to support financial inclusion initiatives. It will not however improve certainty about the true identity of the users of those products.

In the longer term, answers lie in improving national identification systems and in embracing identifiability in relation to appropriate new payment methods, such as mobile money. The starting point of the journey towards an improved system lies however in recognizing the weaknesses of the current approach.

Figure 1

Particulars	Fiji	Malawi	Namibia	Peru	Philippines	South Africa
Full names	•	•	•	•	•	•
Date of birth	•	•			•	•
Place of birth					•	
Citizenship and/or residence	•		•	•	•	
Government identity number other than tax number[a]		•	•	•	•[b]	•
Residential address	•	•	•		•	•
Village, traditional authority and district of origin		•				
Postal address		•				
Telephone number			•	•	•	
Tax number	•				•[b]	
Occupation or source of income	• Including name of employer or nature of business, if self-employed	•	• Including nature and location of business activities, if any	•	• Including name of employer or nature of business, if self-employed	
Source of funds deposited	•		•		•	
Approximate average monthly income	•	•		•		
Public positions held				•		
Whether the person is a PEP				•		
Purpose and intended nature of the business relationship		•				
Specimen signature	•	•			•	

Table I. Identifying particulars for individual required by different countries for opening a bank account

Notes: [a]e.g. national identity number, passport number, social security, drivers license; [b]the Philippines require a government-issued identity number or a tax number

Source: Alliance for financial inclusion

1. Alliance for Financial Inclusion (2013), Balancing Financial Integrity and Financial Inclusion: Lessons Drawn from Regulatory Experience on Implementing a Risk-Based Approach, AFI, Bangkok.

2. Basel Committee on Banking Supervision (2001), Customer due Diligence for Banks, Bank for International Settlements, Basel.

3. Basel Committee on Banking Supervision (2003), General Guide to Account Opening and Customer Identification, Bank for International Settlements, Basel.

4. Basel Committee on Banking Supervision (2012), Core Principles for Effective Banking Supervision, Bank for International Settlements, Basel.

5. Basel Committee on Banking Supervision (2013), "Sound management of risks related to money laundering and financing of terrorism", Consultative Document, Bank for International Settlements, Basel.

6. Bester, H. , Chamberlain, D. , De Koker, L. , Hougaard, C. , Short, R. , Smith, A. and Walker, R. (2008), "Implementing FATF standards in developing countries and financial inclusion: findings and guidelines", FIRST Initiative, World Bank, Washington, DC.

7. Chatain, P.L. , Zerzan, A. , Noor, W. , Dannaoui, N. and De Koker, L. (2011), Protecting Mobile Money Against Financial Crimes: Global Policy Challenges and Solutions, World Bank Publications, Washington, DC.

8. Dass, R. (2011), "Unique identification for Indians: a divine dream or miscalculated heroism?", Vikalpa, Vol. 36 No. 1, pp. 1-13.

9. De Koker, L. (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, pp. 26-50.

10. De Koker, L. (2011), “Aligning anti-money laundering, combating of financing of terror and financial inclusion: questions to consider when FATF standards are clarified”, Journal of Financial Crime, Vol. 18 No. 4, pp. 361-386.

11. De Koker, L. and Jentzsch, N. (2013), “Financial inclusion and financial integrity: aligned incentives?”, World Development, Vol. 44, pp. 267-280.

12. De Montjoye, Y.-A. , Hidalgo, C.A. , Verleysen, M. and Blondel, V.D. (2013), “Unique in the crowd: the privacy bounds of human mobility”, Scientific Reports, 3, available at: www.nature.com/srep/2013/130325/srep01376/full/srep01376.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+mediaredef+jason+hirschhorn’s+Media+ReDEFined (accessed 27 November 2013).

13. Financial Action Task Force (2009), “Mutual evaluation report: South Africa”, FATF, Paris.

14. Financial Action Task Force (2010), “Money laundering and terrorist financing global threat assessment”, FATF, Paris.

15. Financial Action Task Force (2012), “International standards on combating of money laundering and the financing of terrorism and proliferation: the FATF Recommendations”, FATF, Paris.

16. Financial Action Task Force (2013a), “FATF guidance: anti-money laundering and terrorist financing measures and financial inclusion”, FATF, Paris.

17. Financial Action Task Force (2013b), “Guidance for a risk-based approach to prepaid cards, mobile payments and internet-based payment services”, FATF, Paris.

18. Financial Action Task Force (2013c), “Methodology for assessing technical compliance with the FATF recommendations and the effectiveness of AML/CFT systems”, FATF, Paris.

19. Gelb, A. and Clark, J. (2013), “Identification for development: the biometrics revolution”, working paper 135, Centre for Global Development, Washington, DC.

20. Gold, S. (2011), “The privacy initiative”, Biometric Technology Today, June, pp. 9-11.

21. Harris, A. , Goodman, S. and Traynor, P. (2013), “Privacy and security concerns associated with mobile money applications in Africa”, Washington Journal of Law, Technology & Arts, Vol. 8 No. 3, pp. 245-264.

22. Isern, J. and De Koker, L. (2009), “AML/CFT: strengthening financial inclusion and integrity”, CGAP Focus Note, No. 56, CGAP, Washington, DC.

23. Jentzsch, N. (2012), “Implications of mandatory registration of mobile phone users in Africa”, Telecommunications Policy, Vol. 36 No. 8, pp. 608-620.

24. Kumar, K. and Muhota, K. (2012), “Can digital footprints lead to greater financial inclusion?”, CGAP Brief, World Bank, Washington, DC.

25. Lobosco, K. (2013), “Facebook friends could change your credit score”, CNNMoney, 27 August, available at: http://money.cnn.com/2013/08/26/technology/social/facebook-credit-score/index.html (accessed 20 October 2013).

26. Oxford Dictionaries (2013), available at: www.oxforddictionaries.com (accessed 20 October 2013).

27. Paik, M. (2010), “Stragglers of the herd get eaten: security concerns for GSM mobile banking applications”, HotMobile’ 10, Proceedings of the Eleventh Workshop on Mobile Computing Systems and Applications, 22-23 February, Annapolis, MD, pp. 54-59.

28. SAPA (2005), “Fake passports, IDs a ‘crisis’, News24”, 13 September, available at: www.news24.com/World/News/Fake-passports-IDs-a-crisis-20050913 (accessed 20 October 2013).

29. Sathye, M. (2008), “Estimating the cost of compliance of AMLCTF for financial institutions in Australia”, Journal of Financial Crime, Vol. 15 No. 4, pp. 347-363.

30. Veris Consulting (2013), “The global cost of anti-money laundering compliance survey”, available at: www.verisconsulting.com/documents/brochures/The%20Global%20Cost%20of%20Anti-Money%20Laundering%20Compliance.pdf (accessed 20 October 2013).

Further reading

1. Basel Committee on Banking Supervision (2004), Consolidated KYC Risk Management, Bank for International Settlements, Basel.

About the author

Louis de Koker holds a Chair in Law at the School of Law of Deakin University, Australia. He was formerly the Director of the Centre for the Study of Economic Crime at the University of Johannesburg, South Africa. Louis de Koker can be contacted at: louis@deakin.edu.au