CGAP

FOCUS NOTE

# AML/CFT: Strengthening Financial Inclusion and Integrity

Over the past 30 years, access to formal financial services for low-income people has increased dramatically. However, misguided efforts to reduce criminal behavior threaten to slow the pace of that progress.

International standards on **anti-money laundering (AML)** and **combating the financing of terrorism (CFT)** promote financial integrity and support the fight against crime. However, the inappropriate implementation of these standards—especially in emerging markets—plays a role in excluding millions of low-income people from formal financial services. It can relegate the unserved majority to the informal world of cash, undermining social and economic advancements and denying regulators and law enforcement a key means of strengthening financial integrity: the ability to trace the movement of money.

It need not be this way. Financial inclusion and an effective financial integrity regime can—*and should*—be complementary national policy objectives. International AML/CFT standards have some flexibility, enabling countries to craft effective and appropriate controls. The challenge is finding the right level of protection for a particular financial environment.

Fortunately, a growing body of analysis and positive examples from countries around the world is beginning to point the way. This Focus Note shares insights gained from studying some early experiences.

Building on earlier studies, including a CGAP analysis (Isern et al. 2005), the FIRST Initiative funded a five-country study (Bester et al. 2008) to analyze the effects of AML/CFT regulation on access to finance in Indonesia, Kenya, Mexico, Pakistan, and South Africa.[1] It concludes that AML/CFT measures can negatively affect access to, and use of, financial services if the measures are not carefully designed. The study identifies factors that may intensify this impact, provides approaches on the design of appropriate AML/CFT controls that complement financial access policies, and suggests key design principles for AML/CFT controls. Some of these suggestions are as follows:

- AML/CFT measures should be tailored to the domestic environment and the domestic risks of **money laundering** and **financing of terrorism (ML/FT)**.
- AML/CFT controls should be proportionate to the prevailing or likely risks.
- AML/CFT obligations should be matched to the capacity of both public and private institutions.
- Where institutional capacity is lacking, a plan should be developed to improve capacity and phase in AML/CFT obligations as institutional capacity increases.
- Law enforcement should be reserved as primarily the responsibility of the state, and law enforcement responsibilities should not be unnecessarily shifted to private institutions.

## International AML/CFT standards and financial services for low-income people

### FATF Recommendations

The 40 recommendations of the **Financial Action Task Force (FATF)**, along with its special recommendations regarding CFT, are the international standard for AML/CFT regulations (see Box 1).[2]

Although the recommendations are not legally binding on a country, noncompliant countries risk being regarded as havens for criminals and their illicit proceeds and harming their standing as an investment destination. Financial institutions operating in countries that are in compliance are required to give special attention to dealings with any persons and institutions of a noncompliant country. In practice, this often slows the pace of transactions; it may even lead to a decision to avoid business relationships with those persons and institutions.

The FATF recommendations outline measures that countries, financial institutions, and certain other businesses and professions should adopt to counter ML/FT. Countries are advised to do the following:

1 The study also includes case studies on the United Kingdom, the United States, and the Philippines.

2 See the FATF Web site (http://www.fatf-gafi.org) for the complete set of recommendations and related guidance.

No. 56
August 2009

Jennifer Isern and
Louis de Koker

**Box 1: What is FATF?**

**FATF** is an intergovernmental body that sets global AML/CFT standards, assesses member compliance with those standards, promotes global compliance with the standards, and identifies AML/CFT threats. Its members include 32 jurisdictions and two regional organizations (the Gulf Cooperation Council and the European Commission). FATF works closely with eight **FATF-style regional bodies** in Africa, Asia/Pacific, the Caribbean, Europe, Eurasia, the Middle East and North Africa, and South America, representing the majority of countries in the world. Globally, about 180 jurisdictions have directly endorsed the FATF recommendations.

- Adopt laws that criminalize laundering the proceeds of crime and providing financial or material support to terrorists.
- Establish a **financial intelligence unit (FIU)** to receive, analyze, and disseminate information regarding potential ML/FT transactions or activities.
- Ensure appropriate and effective oversight of financial institutions.
- Cooperate with one another in investigating and prosecuting crimes.

The measures required of financial institutions often have the most direct impact on financial access. For example, financial institutions are required to maintain customer due diligence (CDD)[3] measures, such as the following:

- Identify their customers and verify their identities using reliable, independent source documents, data, or information (in practice, by verifying personal details, such as their names, available national identity numbers, date of birth, and contact information).[4]
- Obtain information on the purpose and intended nature of the business relationship.
- Maintain comprehensive records of customer information and transactions.
- Monitor customer transactions, and file a report with the FIU or other appropriate authorities if funds are suspected to be the proceeds of crime or linked to the financing of terrorism.

Institutions must also ensure that employees understand their legal obligations and that measures are in place to enable the institution, its officers, and its employees to meet their compliance obligations.

AML/CFT laws and regulations are normally enforced with serious penalties, such as large fines and imprisonment. A convicted institution's reputation may suffer; it may lose customers and business relationships and may even lose its license.

## Financial service providers working with low-income clients

FATF recommendations cover a broad range of services and activities, including accepting deposits from the public, providing consumer credit, and transferring money or value in the formal and informal sector. The scope of the recommendations includes financial service providers that serve low-income clients (e.g., the diverse grouping of microfinance institutions [MFIs] and new entrants such as branchless banking operators).[5]

This Focus Note addresses some of the negative impacts of inappropriate AML/CFT controls on the services and client base of these providers. However, well-designed AML/CFT controls also provide them with protection and opportunities. The following are some examples of this:

- AML/CFT controls can help institutions understand their customers better, thereby enabling them to design and market better products and support better customer service in general.

3 Some regulatory regimes and practitioners use the term "know your customer" (KYC) interchangeably with CDD.

4 CDD measures also include the duty to take reasonable steps to identify and verify the identity of a beneficial owner. The beneficial owner is the natural person(s) who ultimately owns or controls a financial services customer (for instance, the individual who owns the majority of the shares in the corporation that wishes to open an account) and/or the person on whose behalf a transaction is being conducted.

5 MFIs include a range of financial service providers that serve low-income clients. Examples include savings and postal banks, financial cooperatives, nongovernmental organizations, associations, community and rural banks, commercial banks with broad retail services, money transfer companies, etc. Branchless banking operators include mobile phone companies (mobile network operators), retail agents, and other companies that provide financial services outside of a traditional bank branch. Branchless banking could use a variety of delivery channels, including mobile phones, payment cards (credit, debit, prepaid), automatic teller machines, point of sale machines, and other existing infrastructure. Depending on the country, MFIs and branchless banking operators may be included in broader banking regulation or may be covered by separate regulation.

- If AML/CFT controls are confined to standard, regulated financial institutions and services, then informal service providers could be left vulnerable, and they may be subjected to a disproportionate amount of criminal abuse.
- Providers find it easier to engage regulated financial institutions that may otherwise avoid doing business with them for fear of ML/FT.
- AML/CFT controls can help strengthen overall anti-fraud controls.

### Risk-based approach to AML/CFT

FATF's recommendations envisage AML/CFT controls that are sufficiently uniform across the globe to prevent displacing ML/FT from one jurisdiction to another. However, countries may follow a risk-based approach when they implement key recommendations. This enables countries to design and implement effective AML/CFT controls that are appropriate to their risks and national context.

FATF encourages countries and institutions to focus their attention and resources on people and activities that pose a high risk of ML/FT (FATF 2007).[6] Countries may decide that reduced or simplified controls are sufficient to safeguard low-risk activities against abuse. If a country finds that some financial services for low-income people meet FATF criteria for exemption, it may even exclude those activities, wholly or partially, from its national AML/CFT regime.

### Guidance for low-capacity countries

FATF recognizes that some countries lack the resources to immediately implement a comprehensive system that effectively regulates all areas posing material risk.[7] For these countries, FATF (2008a) suggests designing controls around their risks as well as their resources. The design process should be supported by political commitment to comprehensive AML/CFT measures and informed by a proper appraisal of institutional capacity and an assessment of the ML/FT risks.

A country's implementation plan for AML/CFT controls may allow for some measures to be phased in or sequenced. Sequencing allows a country to implement key AML/CFT measures while improving its capacity to implement the remaining recommendations.[8]

## Access-friendly AML/CFT controls

Country-specific factors could unintentionally create barriers to financial access. The FIRST study identified the following examples.

### Limitations in identification infrastructure

Identity verification is easier and cheaper when there is a trusted, standardized national identification (ID) system, for instance a system based on national ID cards or a system combining various government and commercial databases. Many countries do not have such a system, and even in nations that do issue ID documents, the documents may not be perceived as reliable.

If there is no national ID system, or if the system lacks integrity, or if the database is not accessible, financial institutions often incur additional costs to verify CDD information. This may cause institutions to withdraw from low-value, lower profit transactions and markets. Furthermore, even countries with reliable national ID systems may fail to cover a significant percentage of low-income people or people in remote rural areas, leaving them without formal proof of identity and/or proof of formal residential addresses.[9]

The dynamic can be even more pronounced with some new business models that could expand access to financial services. For example, in some branchless banking models, clients may register and/or conduct transactions at a distance rather than face to face. These models rely on a minimum amount of client ID information that must then be verified against third-party databases, such as a national ID database or credit bureau databases. If such systems do not exist or if they lack integrity, regulators may not approve the business model.

6 In 2007 FATF issued guidance on the risk-based approach for financial institutions. Similar guidance was since issued for accountants, dealers in precious metals and stones, real estate agents, trust and company service providers, legal professionals, casinos, and money service businesses.

7 FATF defines "low capacity countries" as low-income countries that face challenges such as competing priorities for scarce government resources, a severe lack of resources and skilled workforce to implement government programs, overall weakness in legal institutions, a dominant informal sector, a cash-based economy, poor documentation and data retention systems, and a very small financial sector. See FATF (2008a).

8 Key measures include the criminalization of ML/FT, CDD and record keeping duties, and the reporting of suspicious transaction.

9 FATF does not require institutions to request and verify a customer's address; however, this is common practice in developed countries and is required by some developing countries.

## Limited government capacity

Government capacity to supervise and enforce AML/CFT measures can affect its financial inclusion policy. This is particularly relevant in three areas.

- **Supervision.** With limited capacity, supervisors will tend to supervise entities that are easily accessible—typically the largest regulated entities. They may pay little attention to small, informal, and unregulated institutions. As a result, the compliance cost for supervised institutions will increase, with no similar increase for unsupervised institutions. This may cause well-supervised institutions to withdraw from low-income markets where they compete with unsupervised institutions. It may also lead businesses to seek relationships with well-supervised institutions rather than riskier unsupervised/unregulated institutions.
- **Law enforcement.** Law enforcement deficiencies usually mean that risk assessments are not based on actual information, but instead on hypotheses or international typologies. Without an objective understanding of the risks in their country, regulators tend to "play it safe," often adopting control measures that are more onerous than required.
- **Using AML/CFT controls to advance the formalization of the economy.** AML/CFT controls require financial institutions to disclose client information to authorities to combat ML/FT. However, if this information is used for other purposes, such as combating tax evasion, clients whose tax affairs are not in good order may decide to remain outside the formal financial system.

## Strict application by formal financial institutions

Large formal financial institutions tend to apply AML/CFT controls more rigidly than intended by the regulator. For instance, although national regulations may allow discretionary use of alternative documents to verify customers, institutions tend to limit discretion and the types of documents accepted. When mistakes can lead to vast penalties and costs for the institution (and in some cases, for the compliance officer personally), frontline staff may not be trusted to use discretion and to decide which document is best to verify the details of a particular client.

## Extent of informal financial services

Especially in lesser developed economies, financial services are often provided informally through money lenders, informal money transfer operators, unregistered community finance organizations, and others. Low-income people often prefer to use informal financial services because of convenient locations, familiarity with the institutions and their services, and often fewer restrictions (such as ID requirements). Inappropriate AML/CFT measures can inadvertently push people away from formal financial services or create unnecessary barriers to those who want to begin using formal financial services.

## Linkages to international partners and markets

Countries have varying degrees of openness to international financial markets through cross-border commercial relationships, cross-border transactions, and foreign ownership of domestic institutions. Countries with more openness are likely to face more direct and indirect pressure to adopt AML/CFT controls that reflect those implemented by their main international investors and trading partners. The recommendations guide financial institutions to ensure that AML/CFT principles are applied to their branches and majority-owned subsidiaries located abroad, especially in countries that do not apply or insufficiently apply FATF recommendations.[10] As a result, foreign parent companies often require domestic financial subsidiaries to implement controls that are designed abroad. If those controls are stricter than required by the ML/FT risks of the particular country, they may undermine its financial inclusion policy.

## Policy approaches and recommendations

Several countries designed their AML/CFT laws to minimize unnecessary adverse affects on financial access and to promote both financial inclusion and financial integrity. Drawing on initial experiences in these countries, the FIRST study identified several measures that facilitate the design of appropriate

10 Application in remote branches and subsidiaries must be done to the extent that local laws and regulations permit. If such implementation is prohibited, financial institutions should advise competent authorities in the country of the parent institution that they cannot apply the FATF recommendations (Recommendation 22).

### Box 2: Different risks for institutions serving low-income people

A risk assessment may show that the risk profile of financial service providers working with low-income customers is relatively low and justifies simplified AML/CFT measures or even an exemption from measures that would otherwise create unnecessary barriers to access. The risk profile of such institutions may be lower because of the following:

- Clients are generally natural persons (not complex corporate clients where ultimate control can be obscured).
- Providers traditionally have a more personal relationship with their clients and know far more about their clients' activities than standard financial service providers. This knowledge enables the provider to detect and prevent abuse.
- The transactions normally involve relatively small amounts, making them less attractive for large-scale abuse.

Of course, these factors do not mean that there is no risk of abuse. Smaller institutions may not have adequate control systems, exposing them to potential abuse. Money launderers and terrorism financiers often split large transactions into several smaller transactions, schemes referred to as "splitting," "smurfing," or "structuring."

Financial service providers working with low-income clients may be targets of very small structured transactions (micro- or nanostructuring). However, the coordination and effort involved make this relatively unattractive. Transaction limits or caps appropriate to a low-income market and/or monitoring of transactions can reduce the risk even further.

Different types of financial services have different risk profiles. Cross-border money transfer services may pose a higher risk than domestic transfers. Likewise, payment services normally pose a higher ML/FT risk than microcredit services, because the receiving party may not be personally known to the service provider, and the provider often knows less about the sender than a lender knows about its customers.

The potential for abuse also varies by institution and provider type. For instance, a bank that offers microfinance services may have a world-class risk management system to mitigate its risks. A small MFI may have a limited customer base and may know each of its customers by name. Both providers may therefore have adequate measures in place and, as a consequence, a lower risk of ML/FT abuse.

national AML/CFT controls that support financial inclusion. These measures work best when used together and within a comprehensive policy framework.

In the examples presented here, implementation of the approaches is considered to be work *in progress*. The examples are not used to illustrate proscriptive measures but rather to highlight some experiences to date.

## Develop a policy to support effective and proportional AML/CFT controls and financial inclusion.

Many government agencies and departments are involved in different aspects of the AML/CFT framework and of financial inclusion. The core business of these agencies and departments often give them very different perspectives on AML/CFT approaches, policies, and priorities. To ensure a cohesive approach, the country should adopt a clear, overarching policy that commits the government as a whole to effective and proportional controls. The policy should be comprehensive and reflect the approaches outlined in the following.

## To get the right balance, consult with the private sector and other key actors.

To ensure that the AML/CFT framework is addressing appropriate risks while supporting financial inclusion, it is critical to consult financial service providers, law enforcement agencies, financial regulators, the FIU, and other key role players. Because financial security and financial access are ongoing concerns, these discussions also should be ongoing.

It is especially important to engage those who are knowledgeable about social exclusion, financial inclusion, and informal financial services. Unregistered financial service providers, social welfare providers, ID agencies, and credit bureaus have important perspectives to share about ML/FT risk and appropriate risk control measures.

## Assess the specific ML/FT risks of your country.

A risk assessment helps governments design appropriate and proportional AML/CFT controls. It attempts to determine the nature and scale of ML/FT in the country as well as vulnerabilities in existing controls (FATF 2007, FATF 2008c). Developing countries with low capacity should find a risk assessment particularly useful because it will help them to use their limited resources to address key risks (FATF 2008a).

In practice, assessments tend to focus on high-risk activities. However, governments need balanced risk assessments that consider the relative risks and vulnerabilities of high-, medium-, and low-risk activities (De Koker 2009a). It is especially important to develop an informed view of the nature and the relative level of risk posed by financial services typically available to low-income clients. Information sources include government and development agencies and formal and informal financial service providers. Risks categorized by financial subsectors, institutions, transactions, client groups, and other relevant characteristics (e.g., geographic area) will help governments formulate proportional risk-control measures. Risk assessments should be done regularly and should be accompanied by an assessment of the likely impact of proposed AML/CFT controls on service providers and clients.

## Understand the causes and impact of financial exclusion.

To understand the potential impact of AML/CFT controls on financial inclusion, policy makers should understand the main causes of exclusion and the main groups affected. In many countries, a significant percentage of the population is unbanked. Often, a large percentage of the population comprises low-income people, rural and periurban residents, and informal or undocumented migrants.

## Assess available resources to implement AML/CFT controls.

To ensure effective implementation of AML/CFT controls and support for financial inclusion, policy makers should assess the capacity of financial service providers and financial sector regulators, as well as the coverage and integrity of the country's ID system.

Careful analysis can help a country design controls around the existing capacity of the relevant government agencies and service providers:

- Indonesia's AML provisions regarding transaction monitoring take into account the level of technical ability of financial services providers, **requiring that they have an information management system (MIS) in place**, but not prescribing any

### Box 3: Causes of exclusion

It is important to look at the size of the country's informal sector and understand why clients are excluded:

- **Clients denied access.** Lack of physical access to service points may prevent people from seeking formal financial services, especially in rural areas or locations with few branches, automatic teller machines, or other ways of accessing an account. Affordability is another barrier; it includes minimum balances for deposit accounts imposed by financial institutions, account fees, transaction fees, and other costs of using the product. Finally, regulatory barriers, such as ID requirements based on documents that are not freely available to low-income people, may block access.
- **Clients opting out.** People may opt out of formal services if they see more benefits, in terms of cost, convenience, confidence, or cultural links, in going to informal financial service providers. Often, informal services are perceived as less costly, requiring less documentation, conveniently located and welcoming to this market segment.
- **Market inefficiency.** Formal financial institutions may not yet see a market advantage to providing access, or they may be discouraged from expanding their clientele by regulatory burdens. At the same time, informal financial institutions (e.g., NGOs, associations, etc.) may not be allowed to receive licenses, or access other benefits of the formal financial sector if appropriate regulations are not available.
- **Regulatory costs.** Providers may exit markets and potential providers may be barred from entering a market if the regulatory compliance costs are too high. If there are fewer providers, customers may find it more difficult to access appropriate products at an affordable price.

### Box 4: How to assess capacity

The following questions can be posed to help assess a country's capacity to implement appropriate AML/CFT controls:

**Capacity of financial services providers**
- Are information and management systems manual or electronic? Are they appropriate to the institutions' operations?
- Can transaction limits, product restrictions, and monitoring for suspicious transactions be supported by software?
- What customer information is generally available?
- What is the institutions' current and feasible reporting capacity?
- What compliance requirements are already being met? What is the capacity for increased compliance measures?

**Capacity of financial sector regulators**
- Which agencies are mandated to regulate and implement AML/CFT controls? What is—and should be—their reach?
- Is coordination effective among agencies?
- Do the agencies have adequate experienced staff, training, systems, and budget?
- Does an FIU exist? What is its capacity and resources?

**Capacity of national ID system**
- Is there a national ID system or sources of ID information?
- What percentage of the population is covered by the system?
- What factors limit people from obtaining an official ID document?
- What is the integrity of the system? How can risks be mitigated?
- Does the agency responsible for national identification have adequate experienced staff, training, systems, and budget?

particular type or level of technology. Where appropriate, even manual systems are allowed, which is particularly helpful for small institutions that lack technical MIS capacity but are able to monitor transactions effectively through a manual system.

- South Africa's AML/CFT system required financial institutions to identify and verify all their existing clients in accordance with the new rules within 12 months from the date the CDD obligations took effect. Long-standing clients who were not identified in accordance with the new rules risked having their accounts frozen. Clients and institutions struggled to comply, and banks found it very costly to meet such a tight deadline. The government therefore **adjusted the timeline for identifying clients based on risk**. Financial institutions were required to meet the CDD requirements for higher risk clients first, but were given two additional years to complete the procedures for lower risk clients.

## Develop AML/CFT controls proportional to lower risk transactions and providers.

Where the risk of ML/FT is lower, countries can use the flexibility built into the FATF recommendations to design approaches that do not impede financial access. A proportional approach could include modifying client documentation and verification requirements, simplifying complex record keeping requirements, and launching new service channels.

**Client documentation and verification.** Low-income customers often maintain small account balances and conduct low-value domestic transactions that present lower risk for ML/FT. Several countries have adopted proportional controls for these accounts and transactions, where customers are exempted from some of the more onerous standard controls. If customers wish to conduct higher value transactions above a specific threshold, they are then required to comply with full standard verification requirements.

Where risk is lower, reduced controls can facilitate financial inclusion. South Africa introduced a compliance exemption (Exemption 17) that **relaxes its residential address verification requirement** for those bank clients who hold low account balances (under US$ 3000), who conduct small transactions, and who do not conduct international transactions. These "mass banking clients" were considered relatively low risk even though it is typically difficult to verify their residential addresses. A recent study investigated the criminal abuse of these products. It found that while some abuse did occur, the level of abuse was substantially lower and the amounts involved were much less compared to the abuse of standard, non-exempted products (de Koker 2008b).

### Box 5: Potential proportional controls for client identification

Proportional controls, such as the following, might be considered for lower risk clients:

- Allow verification from a range of documents available to low-income people that matches the low risk of ML/FT abuse.
- Simplify verification for low-value transactions under a specified threshold. For example, clients may not be required to show proof of address or may be allowed to use alternate forms of identification to conduct a transaction below a specified limit.
- Focus on client profiling, especially where the national ID system is absent or weak. Where an institution collects additional client information, such as the person's source of income, the intended use of the account, additional contact particulars, etc., it can draw a profile of that client and form an impression of the transactions that can be reasonably expected. That profile can be used to build the client relationship and monitor for suspicious transactions. Improved monitoring of the account on the strength of the client profile may offset risks introduced by simplified verification requirements.
- Allow verification of information through reliable third-party databases, such as credit information registries (credit bureaus) and government databases.

**Record keeping for financial service providers.** Requiring advanced MIS and paper copies of client verification and transaction records will increase costs of compliance and especially affect smaller institutions. Flexibility on MIS requirements could include allowing paper-based or simplified electronic MIS that meet AML/CFT reporting requirements, particularly for smaller institutions with limited numbers of clients and branches.

**Branchless banking using new technologies and business models.** Some new approaches, such as mobile phone banking,[11] present specific risks, but they also allow advanced MIS to facilitate even more comprehensive client and transaction monitoring.[12] Given the readily available information on transactions from mobile banking, flexibility on other controls may be reasonable. One option for domestic low-value transactions through mobile phone banking is to employ authorized agents who verify customer identity for new accounts. Another option is that taken by South Africa, which approved nonface-to-face client registration within the limits of Exemption 17. A bank offering the mobile phone product is required to obtain a name and a national ID number from the client and then cross-reference these against an acceptable third-party database and undertake additional electronic CDD measures. However, since the regulator feels this model introduces higher AML risk, clients who use the nonface-to-face registration process cannot transact against their accounts for more than R1,000 (US$120) a day. Given the unknown nature of the risk, the regulator therefore chose to **limit the functionality of the account rather than to prohibit the business model**. The control measures also allow for flexibility: clients who wish to transact for larger amounts can be released from the restrictions after submitting to regular face-to-face CDD procedures. (South African Reserve Bank 2008).[13]

Through ongoing consultation and monitoring, these proportional AML/CFT controls can be refined as risk and market conditions evolve.

## Phase in AML/CFT implementation, where necessary.

All countries should strive to meet FATF standards within a reasonable time and should ensure that primary processes are in place before secondary processes are imposed. If processes are not properly aligned, controls may be costly but have only limited effect.

Countries that do not have the resources to effectively regulate all areas of potential risk can use a risk-based and sequenced approach.[14] Implementing AML/CFT

11 Mobile banking is a subset of branchless banking. This business model presents distinct AML/CFT issues because of the portability of the device, ability to track the movement of particular SIM cards, and increased information to monitor and link financial and telecommunications transactions.

12 See Chatain et al. (2008) for an in-depth discussion of mobile phone banking and AML/CFT issues.

13 Identification requirements for mobile phone users were introduced in mid-2009. These requirements (in terms of the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002, as amended) are less flexible than the mobile banking measures and pose a challenge to transformational mobile banking in South Africa.

14 See FATF (2008a).

**Box 6: Mitigating ML/FT risks from mobile phone services**

Mobile phones hold great potential to increase financial access, but they are also potential channels of criminal activity. To balance perceptions against the fear of over-regulation, actual risks—rather than perceived risks—need to be identified using the following approaches:

- **Focus on services, not providers.** The lines differentiating financial providers in the banking, telecommunications, credit card, and mobile commerce sectors have become blurred. But the potential risks of mobile phone and payment systems operators more likely depend on the characteristics and complexity of services provided than on the service provider. A service-based approach is also more conducive to creating a level playing field for providers of all types.
- **Differentiate AML/CFT measures among four major types of mobile financial services.** The four core mobile financial services are mobile financial information (m-fINFO), mobile bank and securities account (m-BSA), mobile payment (m-Payments), and mobile money (m-Money). These services are often provided jointly and, in some instances, one acts as a foundation for the others. The less the service models have in common with traditional financial service models, the more their associated risks and their potential to increase financial inclusion. M-fINFO has the most in common with traditional models while m-Money is the furthest removed.

Source: Chatain et al. (2008)

controls based on risk, country context, and capacity of regulators and financial service providers is the most effective approach. AML/CFT controls can be phased in for nonregulated providers, building on these four increasing levels of responsibility and control measures:

**Level 1: Require basic nonprudential registration of financial service providers.** This is a first step for institutions that have not been publicly regulated or previously supervised.

**Level 2: Ensure traceability of clients and transactions.** Requiring client identification and standardized client records will enable supervisors and investigators to trace transactions if needed. This is appropriate for community-based institutions and institutions with no previous experience with supervision.

**Level 3: Increase requirements for client profiling, verification, and monitoring.** As institutional capacity increases, requirements can be added commensurate with the institution's product and client risk levels. This is typically appropriate for institutions that have a history of financial sector supervision.

**Level 4: Enhance verification and interdiction.** Where the national system allows a high level of client verification and transaction monitoring, suspicious transactions may be interdicted by law enforcement before they are finalized. This level of control is appropriate only where institutions and regulators have extensive capacity.

## Promote market-based reforms to encourage people to seek formal financial services.

Policy makers should promote measures that (*i*) allow informal financial service providers to formalize and (*ii*) encourage clients to migrate to formal providers. Clients who move to formal providers generally benefit from greater consumer protection, including certainty and proof of transactions. The financial sector benefits from a more stable system and formal intermediation of deposits and loans in the economy. Policy initiatives that promote financial inclusion and support AML/CFT controls include the following:

- Create simplified nonprudential registration or licensing procedures for informal financial service providers, especially those serving low-income clients.
- Encourage codes of conduct for formal financial service providers to increase their visibility and level of service to low-income clients.
- Reduce the incentives to use informal channels, for instance, exchange rate policies that may influence client behavior.
- Facilitate the use of formal financial services by undocumented migrants, especially for remittances and money transfers.
- Encourage new market entrants that have cheaper and more convenient business models, such as mobile banking and the use of nonbank agents.

A government can encourage people to use formal financial services and create an environment that facilitates access to financial services. It is, however, difficult to change consumer behavior patterns. Examples of government efforts include formalizing remittances and tying inclusion to private sector incentives:

- The Indonesian government tries to protect migrant workers by encouraging them to use formal financial services. It **requires migrant workers to open a formal bank account before working abroad**. This approach has had some success; however, many workers still use informal services because they struggle to meet documentation requirements in the sending country and/or because they prefer to carry cash home with them.
- Pakistan has a high inflow of remittances, and the State Bank of Pakistan has done much to increase the flow of remittances through formal channels by **reducing transfer costs and ensuring better official exchange rates**.
- As one of the top three remittance-receiving countries in the world, Mexico has been an active facilitator of remittance flows. The Mexican government has **lobbied hard for U.S. institutions to accept the Matricula consular card as proof of identity** for Mexican immigrants who lack formal U.S. residency documents. Because of these efforts, it is estimated that as much as 90 percent of the remittances between the United States and Mexico flow through formal channels.
- The South African government, in conjunction with the business community, labor, and community constituencies, created the conditions in which the South African financial services industry adopted the Financial Sector Charter in 2003. The Charter committed the banking industry to providing basic banking services to 80 percent of lower income clients. **The ability to secure government contracts is tied to these social targets, so institutions have an incentive to reach them.** The Charter was a major policy intervention that spurred banks to cooperate in offering a highly successful basic bank account, the Mzansi account. More than 6 million of these accounts were opened to date.

## Develop the national ID system.

While a national ID document is not a precondition for an effective AML/CFT framework, the absence of reliable ID documentation or accessible verification sources complicates CDD processes, increases compliance costs, and undermines the effectiveness of AML/CFT controls. To address shortcomings in the national ID infrastructure that might pose barriers to financial access, there are several early examples of innovative AML/CFT controls that do not impose overly burdensome requirements:

- Most Indonesian adults have a national ID card. However, these cards are not issued centrally, and various institutions issue acceptable forms of identification. A person may have more than one ID document, and the information on them may differ. Concerns about corruption and ease of falsification further undermine the integrity of the documents. Nevertheless, the ID card is accepted for CDD purposes because it is the best available means of identification. Indonesia requires banks to use the information contained on the card and additional information requested from the client to develop **a profile of the client and the client's expected transactions**. Typically clients are asked questions to ascertain their occupation, income, and expected transactional activity, although this information is not verified. Client profiles enable the bank to identify transactions that may be suspicious because they are inconsistent with the client's profile. Profiling is a useful enhancement to the limitations of upfront identification using the card. Meanwhile, Indonesia is taking steps to improve the integrity of its national ID system.
- South Africa has an extensive national ID system, but its general AML/CFT requirement that a client's residential address be verified was a potential problem for a significant number of low-income people who did not have proper documentation (e.g., utility bills, rental agreements). As a result, South Africa modified its AML/CFT regulations, allowing financial institutions to verify a person's identity using the national ID document **without having to verify the person's residential address if the financial product meets a certain balance**

**limit (US$3000) and transaction restrictions (US$600 per day)**. This modest relaxation of the standard CDD requirements, which proved very helpful in increasing financial inclusion, was favorably considered by FATF in its 2009 mutual evaluation of South Africa's compliance with FATF recommendations.

- The United Kingdom is implementing a national ID card system. Currently, a financial institution must obtain a client's full name, residential address, and date of birth. This information is typically verified with a valid passport or photo drivers license and/or by accessing appropriate electronic databases. However, the system allows people who have difficulty meeting the standard requirements and who wish to open a basic banking account to present **alternative documents**. For example, individuals in assisted living accommodations may produce a letter from the facility manager and homeless individuals may produce a letter from an employer or the manager of a homeless shelter.

If the existing ID system lacks adequate coverage or integrity or if it is not easily usable for CDD purposes, government agencies could adopt the following initiatives:

- Define conditions, including reasonable fees, for authorized financial institutions to access existing public databases.
- Ensure that accurate data are collected and stored safely.
- Facilitate the establishment of new databases, such as private credit information registries (credit bureaus), and allow the use of their records for CDD purposes.
- Evolve toward biometric means of ID verification.

Alongside national identification, countries should also ensure that their consumer data privacy rules meet international privacy standards. Unless personal data are protected, clients (and especially unbanked clients) may prefer informal (untraceable) financial services. The right of various government agencies to access the data, must also be considered. For example, potential clients may be reluctant to use formal financial services if their data are accessed by local or national tax authorities.

## Conclusion

The pursuit of financial inclusion and the combating of ML/FT can be—and should be—complementary national policy objectives. When low-income clients are excluded from formal financial services, the goals of the AML/CFT policy cannot be achieved. It is challenging to advance both objectives, but customizing AML/CFT policies to the local context, and implementing them sensitively, can deliver significant benefits to clients and financial services providers.

## Sources


Bester, H., D. Chamberlain, L. de Koker, C. Hougaard, R. Short, A. Smith, and R. Walker. 2008. *Implementing FATF standards in developing countries and financial inclusion: Findings and guidelines.* The FIRST Initiative. Washington, D.C.: The World Bank.

Chatain, P-L, R. Hernández-Coss, K. Borowik, and A. Zerzan. 2008. *Integrity in mobile phone financial services: Measures for mitigating risks from money laundering and terrorist financing.* Washington, D.C.: The World Bank.

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, 26.

———. 2009a. Identifying and managing low money laundering risk: Perspectives on FATF's risk-based guidance. *Journal of Financial Crime,* Vol. 16 No. 4.

———. 2009b. The money laundering risk posed by low risk financial products in South Africa: Findings and guidelines. *Journal of Money Laundering Control,* Vol. 12 No. 4.

Financial Action Task Force. 2007. *Guidance on the Risk-based Approach to Combating Money Laundering and Terrorist Financing—High Level Principles and Procedures.* Paris: FATF.

———. 2008a. *Guidance on Capacity Building for Mutual Evaluations and Implementation of the FATF Standards Within Low Capacity Countries.* Paris: FATF.

———. 2008b. *Terrorist Financing.* Paris: FATF.

———. 2008c. *Money Laundering and Terrorist Financing Risk Assessment Strategies.* Paris: FATF.

Isern, J., D. Porteous, R. Hernandez-Coss, and C. Egwuagu. 2005. "AML/CFT regulation: Implications for the financial service providers that serve poor people". Focus Note 29. Washington, D.C.: CGAP.

Lyman, T., M. Pickens, and D. Porteous. 2008. Regulating transformational branchless banking: Mobile phones and other technology to increase access to finance. Focus Note 43. Washington, D.C.: CGAP.

South African Reserve Bank. 2008. *Cell-phone Banking.* Guidance note 6/2008 issued in terms of section 6(5) of the Banks Act, 1990.

This Focus Note presents key findings of a recent report (Bester et al. 2008. Implementing FATF standards in developing countries and financial inclusion: Findings and guidelines. FIRST Initiative. Washington, D.C.: The World Bank) and provides additional perspectives on issues pertinent to access to finance. The study was financed by the FIRST Initiative and undertaken by Genesis Analytics. Jennifer Isern of CGAP chaired the international steering committee for the study.

The authors of this Focus Note are Jennifer Isern, CGAP Lead Microfinance Specialist, and Louis de Koker, CGAP Policy Advisory Consultant and Professor of Law, Deakin University, Australia. They are grateful for helpful comments on the draft paper from Latifah Merican, Stuart Yikona, and Emiko Todoroki of the World Bank Financial Integrity Unit and Rich Rosenberg, Tim Lyman, Jeanette Thomas, Michael Tarazi and Anna Nunan of CGAP.

The suggested citation for this Focus Note is as follows:
Isern, Jennifer, and Louis de Koker. 2009. "AML/CFT: Strengthening Financial Inclusion and Integrity." Focus Note 56. Washington, D.C.: CGAP.

The Financial Sector Reform and Strengthening (FIRST) Initiative is a multi-donor grant facility providing technical assistance to low- and middle-income countries to promote financial sector development. Technical assistance grants from FIRST enable national policy making and regulatory bodies to define strategies, sharpen policies, improve legal frameworks, build domestic financial markets, and strengthen capacity to regulate, supervise, and develop the financial sector in their countries.

FIRST initiative
Strengthening Financial Sectors

Please share this Focus Note with your colleagues or request extra copies of this paper or others in this series.

CGAP welcomes your comments on this paper.

All CGAP publications are available on the CGAP Web site at www.cgap.org.

CGAP
1818 H Street, NW
MSN P3-300
Washington, DC
20433 USA

Tel: 202-473-9594
Fax: 202-522-3744

Email:
cgap@worldbank.org