



The views expressed in this whitepaper are those of the author and are not associated with the views of any other person or company.

ML is the process of converting black money (money from illicit transactions) into white money (money untraceable to any criminal activity).

FT is the means for terrorists to move money and finance terrorist activity.

Reserve Bank of India circulars can be found on www.rbi.org.in

AML circulars are

[DBOD.AML.BC.No.-](#)

[63/14.01.001/2007-08](#) and

[DBOD.NO.AML.BC.28/-](#)

[14.01.001/2005-06.](#)

Account opening and KYC

circulars are [DBOD.No.BL.BC.-](#)

[58/22.01.001/2005-06](#) and

[DBOD.No.Leg.BC.44/09.0-](#)

[7.005/2005-06](#) and

[DBOD.No.Leg.BC.28-](#)

[/14.01.001/2005-06](#)

The FIU website is fiuindia.gov.in.

Three Tools

KYC is the evaluation of a customer to ensure s/he is not a criminal and will not engage in illicit activity. This is often performed through verification of identification documents.

SAR uses pattern recognition to identify suspicious transactions and report these to agencies such as FIU for further investigation.

Usage Limits are implemented into the design of a product to create maximum or minimum limits on financial activity.

Financial services have always been highly regulated to prevent Money Laundering (ML) and the Financing of Terrorism (FT). In India there are Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) regulations and a Financial Intelligence Unit (FIU) to create a strong foundation for Indian financial safety.

The AML/CFT goals create financial exclusion in two different ways. The first kind of exclusion occurs when security measures mandated by law are costly enough to make certain low income (and low profit margin) sections of the population unprofitable for service providers. The second type of exclusion occurs when certain individuals cannot pass verification procedures because they lack certain formal documents.

Contrary to perceptions, AML/CFT goals need not impede financial inclusion. The most successful systems are built upon the principle that security and financial inclusion can with innovation support and further each other. The purpose of the paper is to suggest innovative, prudent and pragmatic regulation that can make Universal Financial Access (UFA was introduced in Whitepaper #1) a reality and at the same time contribute towards the battle against ML and FT.

Three Tools and Four Approaches (For three tools see sidebar)

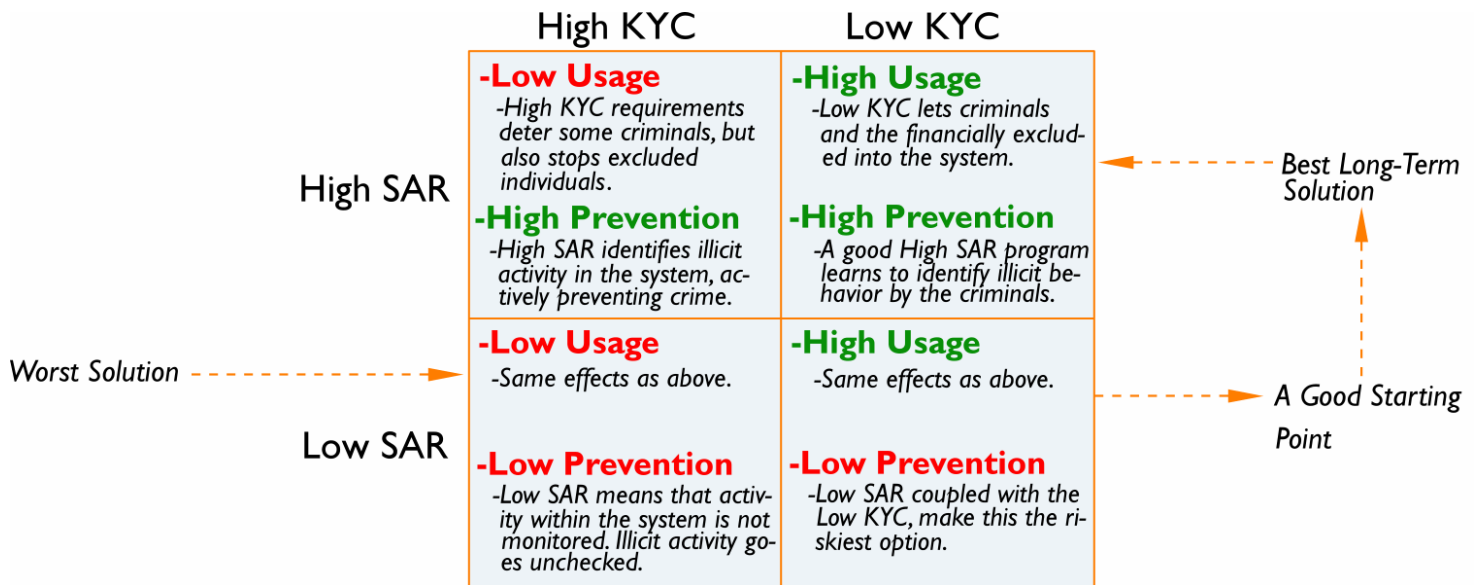
The three tools used to fight ML and FT are Know Your Customer (KYC), Suspicious Activity Reports (SAR) and Usage Limits. KYC is used to try and prevent criminals from initially entering the system, SAR monitors activity and reports suspicious patterns while Usage Limits seek to limit the damage a person who has breached the other defenses can do. KYC and SAR are used to design the system so we will discuss them in the next few sections. Usage limits act as an overlay on the design and will be discussed later.

KYC and SAR

While KYC and SAR are effective tools, over zealous KYC application has created excessive costs to financial institutions which in turn have made financial products too costly to offer to low income Indians. In addition, KYC has excluded those without government documents. Due to the negative consequences of KYC and the intricate nature of a potentially successful SAR program, the following is a description and reasoning of how to best implement them both for optimum security.

Four Design Approaches

To display the dynamic effects of KYC and SAR, the following pictorial shows all the possible implications of creating a financial product with high or low amounts of KYC and high or low amounts of SAR (pattern recognition).



The negative realities of KYC are conveyed in the pictorial. The desire to have robust KYC is often manifested through document checks, but in many countries fake documents are readily available. In many cases the financially excluded do not even have verifiable government documents. The best long term solution is to let in the criminals and the financially excluded together, and then let SAR determine who is performing illegal activities through pattern recognition.

Surprisingly the best system to start with is actually the riskiest model (Low SAR and Low KYC). This approach is counter intuitive and I can see lot of regulators and auditors having trouble digesting this. However, if you think with an open mind and want to make your system very ease to use for the honest user then you do not want to generate too many false positives. Frequent false positives will add to honest user pain and also increase costs by investigating too many leads.

But why should you choose the riskiest model to start? Because at a products inception, the aggregate amount of money that it moves is very low. It is then that an enterprising company must implement Low SAR and Low KYC to learn more about all the possible fraud schemes its system is susceptible to. Because the aggregate flows of money are less at this point, the inevitable fraud will result in low and acceptable losses. In the long run, once the High SAR and Low KYC regime has been implemented, the SAR programs and pattern recognition systems will have learned a tremendous amount from the initial period of high risk exposure. By opening up the system to fraud first, the pattern recognition system can learn about possible fraud scenarios and make the system healthier in the long run.

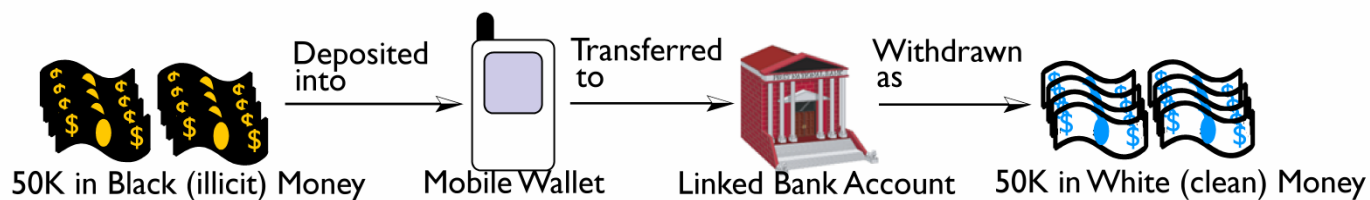
The importance of SAR

In many cases, even when KYC is high, it can fail to protect a system. Consider the following company and the resulting methods of fraud that can occur. The example shows how KYC and Usage Limits can only do so much to stop potential fraudsters, and that SAR techniques are better at securing systems, providing early warnings and also potentially catching criminals.

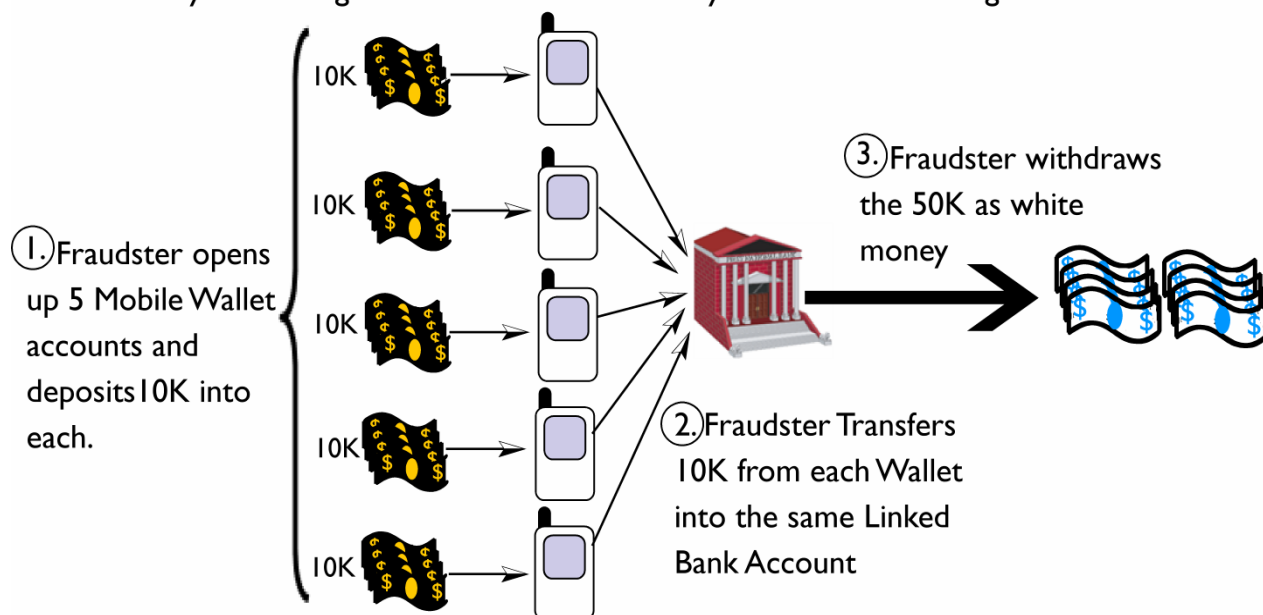
A company named MobileMoney has just offered a "Mobile Wallet" application for users to perform simple banking transactions (deposit, withdraw and transfer money to other MobileMoney users) over their cell phones. To sign up, customers must either:

- OR
- Pass KYC inspection (document, background checks)
 - Link an existing bank account to their Mobile Wallet and KYC will be satisfied through Piggybacking*.

1. How a fraudster could abuse the Mobile Wallet application to perform Money Laundering:

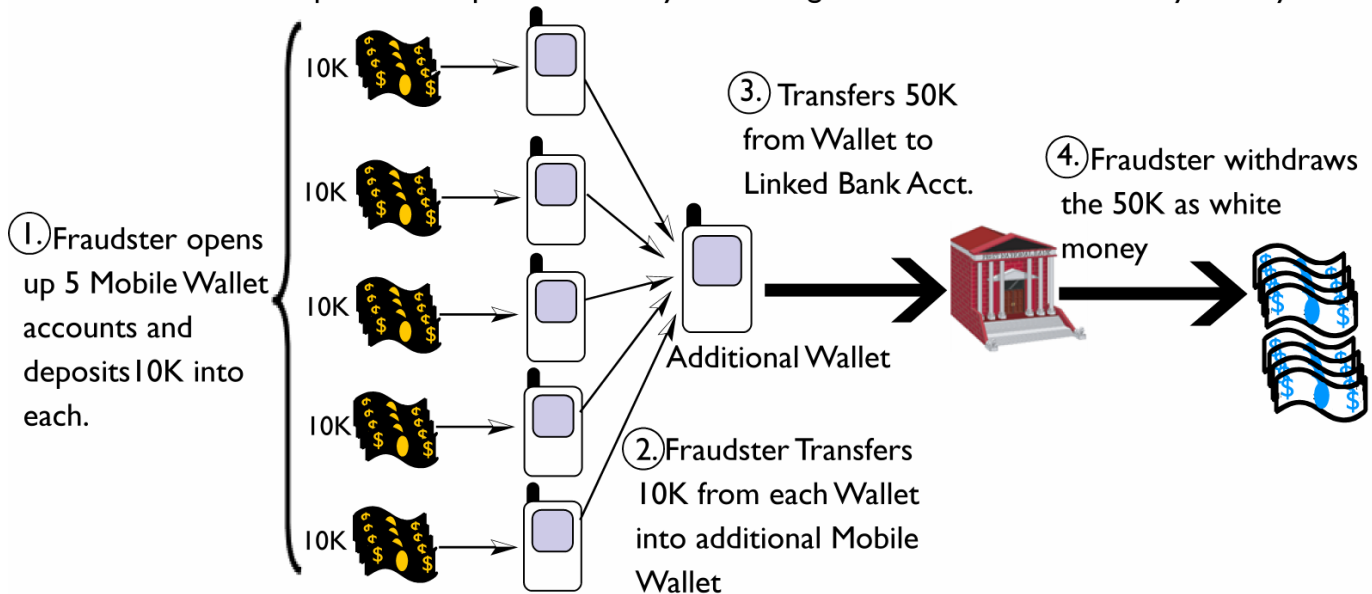


2. MobileMoney institutes a 10K deposit limit on the Mobile Wallet in an attempt to prevent large scale money laundering. The fraudster breaks the system in the following manner:

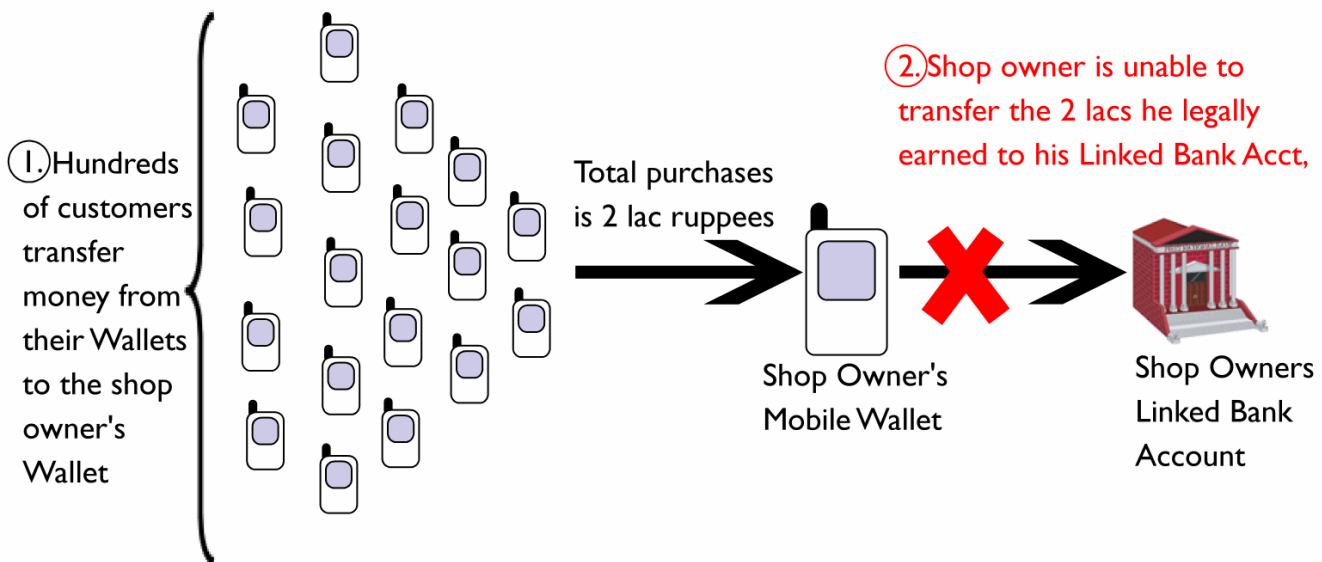


***Piggybacking** refers to where the mobile wallet is linked to a bank account/ credit card in a manner where the system is sure that the linked account or credit card belongs to the mobile wallet user as well. Because the user has already been through KYC to get the card/account opened, KYC is not required again for the mobile wallet. (M-Check and PayPal both use Piggybacking)

3. MobileMoney then decides to additionally stipulate that only one Mobile Wallet can be linked to any one Bank Account to prevent the previous money laundering. The fraudster breaks the system by:



4. To combat the opening of multiple Mobile Wallets, the bank limits the total transfer amount allowed to a linked bank account. This is successful in deterring money laundering, but now a shop owner cannot use Mobile Wallet to conduct business:



Clearly Usage Limits and KYC can only go so far to protect the "Mobile Wallet". To truly be secure and provide inclusion simultaneously, SAR (pattern recognition) technologies must be used to spot suspicious activity instead. In the example above, if the normal level of financial activity for the shop owner is known and the pattern of cash movement into the account is displaying unusual variations that look like ML, then a suspicious activity report can be filed and the situation would be further explored.

Criminals avoid systems with high detection probability

The arguments against high KYC systems have so far been because of their cost ineffectiveness and exclusionary tendencies. In addition, adopting the suggested approach (with Low KYC and High SAR) will build a system that poses a high detection risk for criminals through the advanced SAR (pattern recognition). Creating a system which increases inclusion but does not compromise security is ultimately the goal of innovative, prudent and pragmatic regulation.

Designing the Ideal System

In an Indian context, it would make most sense to create a financial system with reasonable usage limits, simple KYC and robust SAR modules. As previously shown, such a system could successfully promote financial inclusion while providing added financial security. The tools of usage limits, KYC and SAR should be designed with the following in mind.

(The suggestions described below should not be taken as final and optimal for all contexts. It should rather encourage innovators to use some of these principles to build systems which achieve inclusion and low usage by fraudsters.)

Simple KYC

1. *Piggybacking.* People who have bank accounts should be able to link their accounts through verifiable methods. In this case, KYC does not need to be repeated, as long as the verification process is secure.
2. *Minimum Requirements.* Customers who do not have bank accounts should be able to provide a voter ID card or fill out an application to get a voter ID card in order to open an account. Till the voter ID card is issued, their accounts must be subjected to restrictive usage limits.

*By asking people to sign up for **Voter IDs** if they have no identification, India can solve two issues at once. Provide secure financial inclusion and increase the eligible voter base.*

Usage Limits

1. *Receive, Deposit, Withdraw (Minimal Functionalities).* For accounts that can only deposit money, withdraw money and receive but not send transfers, there is zero risk of Money Laundering. This is an important account concept because for the majority of Indians who receive remittance money, or just need a simple savings account, this is all the functionality they will want.
2. *System Limits:* Initially it would be prudent to have limits on the total amount of money that can be moved through the financial products system. When the system is moving less amounts of money, it becomes easier to catch fraud.

Robust SAR

1. *A Secret Formula.* Much like Google and Coca-Cola, the pattern recognition systems must use secret formulas to derive their success. If fraudsters and terrorists understand the systems tracking them, they will have gained an

*When the system is moving smaller amounts of money, small losses does not mean much. It could just be that fraudsters have not deemed the system worth attacking. This is where **ethical hacking** can keep up with the new fraudsters.*

advantage

2. *Ethical Hacking (See Sidebar)*. A technique that is commonly used to improve SAR systems is called ethical hacking. A company or government hires professional hackers to break the security systems and report how it was done. In this way, SAR techniques can stay multiple steps ahead of the fraudsters trying to break the system and adapt continuously.

Innovative, Prudent & Pragmatic Regulation for a Brighter Indian Future

The road to innovative, prudent & pragmatic regulation will be very long if financial inclusion and security are not built with considerations for each other. The costs that restrictive regulations can bear upon a financial system and economy are too great to let the issues go unsolved. The three tools that are currently used to solve AML/CFT regulations can either be implemented with security *and* financial inclusion in mind, or they can be applied without considering their consequences for the financially excluded. Considering that the current realm of the financially excluded contains upwards of 300 million working Indians we do not have a choice. We must include them.

By using this whitepaper to question traditional methods and encourage innovation, we can bring India one step closer towards financial inclusion.