Washington Journal of Law, Technology & Arts

Volume 8
Issue 3 *Mobile Money Symposium*

Article 12

1-1-2013

The Reporting of Suspicious Activity by Mobile Money Service Providers in Accordance with International Standards: How Does It Impact on Financial Inclusion?

Miriam Goldby

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 8, ISSUE 3 MOBILE MONEY SYMPOSIUM 2013

REPORTING OF SUSPICIOUS ACTIVITY BY MOBILE MONEY SERVICE PROVIDERS IN ACCORDANCE WITH INTERNATIONAL STANDARDS: HOW DOES IT IMPACT ON FINANCIAL INCLUSION?

Miriam Goldby[*]

Cite as: 8 WASH. J.L. TECH. & ARTS 401 (2013)
http://digital.law.washington.edu/dspace-law/handle/1773.1/1205

ABSTRACT

Among the obligations which countries are required to impose upon their financial institutions under the Financial Action Task Force's (FATF) 40 Recommendations is the obligation to report suspicions of money laundering. This Article discusses the impact that a reporting regime such as that set up in the United Kingdom in response to FATF requirements is likely to have should it be set up in developing countries seeking to regulate mobile money services. This Article argues that certain features of the U.K. suspicious activity reporting regime make it unsuitable for wholesale adoption into such a context. A one-size-fits-all approach by the FATF in establishing suspicious activity reporting obligations is likely to reduce the accessibility, affordability and attractiveness of mobile

---

[*] Lecturer in Insurance and Commercial Law, Centre for Commercial Law Studies (CCLS), Queen Mary, University of London. Thank you to Prof. Louis de Koker and Prof. Jane K. Winn for their input in the writing of this article and their comments on earlier versions of it. Thank you also to Laura Powell for her assistance in editing and proofreading. Any remaining errors or omissions are purely my own.

This Article was presented at the Mobile Money in Developing Countries: Financial Inclusion and Financial Integrity Conference held in April 2012 at the University of Washington School of Law with the support of the Linden Rhoads Dean's Innovation Fund.

money services, thus impacting negatively upon the goal of financial inclusion.

TABLE OF CONTENTS

INTRODUCTION

This Article seeks to draw upon the author's research on the United Kingdom's Suspicious Activity Reporting (SAR) Regime in order to establish some preliminary points of discussion regarding the impact that a similar regime is likely to have in developing countries upon mobile money services which have to comply with similar reporting requirements under the international standards issued by the Financial Action Task Force (FATF).[1] SAR regimes are set up in compliance with FATF Recommendation 20, which provides:

> If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report

[1] FIN. ACTION TASK FORCE [FATF], INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION: THE FATF RECOMMENDATIONS (2012), *available at* http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%20(approved%20February%202012)%20reprint%20May%202012%20web%20version.pdf [hereinafter FATF RECOMMENDATIONS].

> promptly its suspicions to the financial intelligence unit (FIU).[2]

Mobile money services have made financial services accessible to millions of people in the developing world who are not able to make use of banking services. Generally the service consists of value being loaded onto and stored in a mobile phone account, the owner of which can then use it to carry out everyday transactions, such as grocery shopping and paying utility bills.[3] The service thus consists broadly of a financial service (the maintenance of an account) and a telecoms service (the transmission of transaction messages to move value to and from accounts).[4] The provider of the financial service (whether or not it is the same person as is providing the telecoms service) will be liable to comply with certain AML requirements, including customer due diligence, suspicious activity reporting and record-keeping in accordance with the FATF Recommendations.[5] In countries where large swathes of the population do not have access to a bank branch, these types of services have revolutionized the way that people manage their finances. Accessibility and affordability of the services are key to the success of the service and to financial

---

[2] *Id.* at 19. The text of Recommendation 20 was previously found in Recommendation 13 and Special Recommendation IV.

[3] *See, e.g.*, FATF, FATF GUIDANCE ON ANTI-MONEY LAUNDERING AND TERRORIST FINANCING MEASURES AND FINANCIAL INCLUSION (2011), *available at* http://www.fatf-gafi.org/media/fatf/content/images/AML%20CFT%20measures%20and%20financial%20inclusion.pdf [hereinafter FATF 2011 GUIDANCE]; PIERRE-LAURENT CHATAIN ET AL., PROTECTING MOBILE MONEY AGAINST FINANCIAL CRIMES: GLOBAL POLICY CHALLENGES AND SOLUTIONS (2011).

[4] See CHATAIN ET AL., *supra* note 3, at 12-14, who divide up the mobile-money service into five elements or functions: (1) mobile communications service; (2) customer interface; (3) transaction processing; (4) account provision; and (5) settlement.

[5] This is in line with the findings of CHATAIN ET AL., *supra* note 3, at 28, according to whom "the provider who manages the account records is in the best position to supervise the AML/CFT procedures of the providers at the other stages, and it may be advisable to place the legal burden for regulatory compliance on that provider. This is because the account records function is where the information about customers, retail outlets, and activity all comes together."

inclusion, a major development goal for these countries.

I. FINANCIAL INTEGRITY REQUIREMENTS APPLICABLE TO FINANCIAL INSTITUTIONS

Under the FATF Recommendations financial institutions are required to comply with certain requirements as to customer due diligence (CDD, which includes identifying the customer and monitoring account activity), record-keeping, and reporting of suspicious activities in order to protect financial integrity when performing transactions for customers. The expression "financial institution" includes any natural or legal person who accepts deposits and other repayable funds from the public by way of business and/or provides money or value transfer services to its customers, by way of business,[6] but does not include "any natural or legal person that provides financial institutions solely with message or other support systems for transmitting funds."[7] It therefore includes mobile money service providers who provide customers with both the financial and the telecommunications services,[8] but not those that simply provide the

[6] FATF RECOMMENDATIONS, *supra* note 1, at 115.

[7] *Id.*

[8] An example of this is O2's Wallet service. O2, a telecoms company, allows its customers to deposit money into their electronic wallet up to a certain maximum per year. This maximum can vary among customers, some being allowed £800, some £5,000, others £10,000. The service will only be provided after CDD has been undertaken and the customer has been approved. *See Finance and Insurance Terms and Conditions – O2 Wallet Agreement*, O2, http://www.o2.co.uk/termsandconditions/finance-and-insurance/o2-money-wallet (last visited Aug. 16, 2012). A similar service, Beem, is provided by Mobile Sense, also a U.K. company. *See Mobile Money*, BEEM, http://www.beemme.co.uk/legal (last visited Aug. 16, 2012). The website indicates that "[y]ou can open a Beem account wherever you are, you don't need to be online. To open on the go just text OPEN to Beem at 07624 81 66 66 and follow the simple text prompts." *Using Beem*, BEEM, http://www.beemme.co.uk/using-beem/account-setup (last visited Aug. 1, 2012). In this case a user is prompted to register a debit card, which provides Beem with a method of verifying the user's identity. The limit allowed on a Beem account is £300 within any thirty-day period. A Beem account does not require linking it to a bank account. In this case the procedure for opening the account seems to differ and may need to be completed online.

telecommunications service (the sending or receiving of messages for effecting money transfers over accounts held with others). This means that in countries where bank accounts are ubiquitous and the mobile service is simply used to send messages instructing the financial institution to effect transactions over these accounts, the mobile communications service provider can avoid being designated a financial institution by simply acting as a conduit for the bank to provide the service.[9] On the other hand the mobile money service provider may itself want to provide the account over which the transactions take place, usually because it is profitable to provide the service in view of high demand. This is particularly true in countries where large swathes of the population do not have access to a bank account. In this case, the mobile money service provider will be subject to anti-money laundering (AML) and counter financing of terrorism (CFT) rules applicable to financial institutions. Because the financial service would be provided on a regular basis, the developing country in question would not be able to exempt these businesses from the FATF requirements applicable to financial institutions.[10]

Ensuring accessibility and affordability of mobile money services while at the same time protecting financial integrity in line with international standards may involve far greater difficulties in developing countries than doing so in the world's advanced economies. The table below gives a brief overview of factors that are taken for granted in advanced economies that may, depending

---

[9] See for example the products and services provided by Monitise, a U.K. company, which appear to consist of messaging services allowing payments to and from bank accounts to be effected over a mobile phone. Monitise does not appear to itself provide financial (as distinct from telecommunication) services. It simply provides the platform over which such messages may be sent. *See* MONITISE AMERICAS, INC., http://www.monitise.com/ (last visited Aug. 16, 2012).

[10] Indeed the exclusion may only apply when "a financial activity…is carried out by a natural or legal person *on an occasional or very limited basis* (having regard to quantitative and absolute criteria), such that there is low risk of money laundering and terrorist financing." FATF RECOMMENDATIONS, *supra* note 1, at 32 (emphasis added). Subsequently, "a country may decide that the application of AML/CFT measures is not necessary, either fully or partially." FATF 2011 GUIDANCE, *supra* note 3, at 20.

on the service in question, constitute obstacles in the developing world.

Accessibility	**AE**[11]	**DC**[12]
Register through existing bank account with local bank	✓	?
Proof of address	✓	?
Proof of identity	✓	?
Smartphone technology	✓	?
Stable internet connection	✓	?
Affordability	**AE**	**DC**
Regulation: ▪ Does not preclude market-entry by new providers	✓	?
▪ Does not make service prohibitively expensive	✓	?

Aware of the obstacles that are likely to arise in the implementation of financial integrity measures, the FATF published a report on the issue in June 2011.[13] This report discusses instances of simplified due diligence which may be applied where there is difficulty in obtaining regular proof of identity and address by establishing alternative methods of verification. It also discusses the potential to apply the general risk exemption,[14] under which financial institutions may be exempted

[11] Advanced Economies.

[12] Developing Countries.

[13] FATF 2011 GUIDANCE, *supra* note 3.

[14] This exemption applies: (a) in strictly limited and justified circumstances; (b) based on a proven low risk of money laundering and terrorist financing, and (c) relating to particular a type of financial institution or activity. Thus the application of the exemption depends on proving low money laundering risk. This could be done using Groupe Spéciale Mobile Association's (GSMA) Methodology for Assessing Money Laundering and Terrorist Financing Risk. *See* Marina Solin & Andrew Zerzan, *Mobile Money: Methodology for Assessing Money Laundering and Terrorist Financing Risks* (GSMA, Discussion Paper, 2010), *available at* http://www.ifc.org/ifcext/gfm.nsf/AttachmentsByTitle/Tool10.11.GSMAMethodology-AssessingAMLRisk/$FILE/Tool+10.11.+GSMA+Methodology+-+Assessing+AML+Risk.pdf. In the Philippines this

from complying with full CDD requirements in respect of certain low-risk products. It gives illustrations of different ways in which proof of identity and address may be obtained in places where people may not be living at a formal registered address and may not be able to provide formal proof of identity. For instance in India for the opening of a certain maximum-balance and maximum annual credits accounts, introduction and certification by an existing account holder or any other evidence as to the identity and address that is to the satisfaction of the bank, can suffice for the purposes of customer identification.[15] Special provision is also made for customers without any acceptable form of identity, such as migrant laborers, opening what are called "small accounts."[16] In the Philippines would-be users of financial services from certain rural areas can produce a Barangay Certificate (i.e., a certificate issued by the elected head of the village) for the purposes of customer identification and residence.[17] An interesting example of the application of the general risk exemption may be found in South Africa where Exemption 17 releases financial institutions from address verification requirements in respect of certain low-risk maximum balance accounts permitting only domestic transactions below a certain value.[18] This exemption has reportedly resulted in the more widespread use of financial services including a mobile money service called WIZZIT.[19]

After the service has been set up and the customer accepted as such, the FATF Recommendations require financial institutions to monitor their customer accounts and report suspicious activity. This places certain burdens on financial institutions and affects their relationship with their customers. Some salient features of the system set up in the United Kingdom in response to FATF requirements and the implications for developing countries

---

resulted in lower customer due diligence requirements for certain low-risk customers of SMART Communications. *See* FATF 2011 GUIDANCE, *supra* note 3, at 23.

[15] FATF 2011 GUIDANCE, *supra* note 3, at 29.

[16] *Id.* at 33.

[17] *Id.* at 29.

[18] *Id.* at 32.

[19] *Id.* at 33.

wishing to promote financial inclusion through mobile money are discussed below.

II. SOME FEATURES OF THE AML REPORTING REGIME IN THE UNITED KINGDOM

While much has been said regarding the difficulties of implementing CDD requirements in developing countries, less attention has been devoted to the problem of SAR. In response to the FATF Recommendations, complex SAR systems have been set up in developed countries whereby suspicious activity reports (SARs) may be prepared and submitted by reporters and accessed and actioned by the authorities. The successful establishment and operation of such a system require the investment of time and resources that may not be available in developing countries. Salient features of the U.K.'s SAR system, administered by the Serious Organised Crime Agency (SOCA) and the difficulties of implementing such a system in a developing country are highlighted below.

As FATF Recommendation 20 suggests, the foundation of any SAR system will usually be legal provisions laying down criminal or administrative sanctions for failure by financial institutions to file reports on suspicious activity (i.e., activity on their clients' accounts which may constitute money laundering). In the United Kingdom the failure to report an offense is enshrined in Section 330 of the Proceeds of Crime Act 2002 (POCA). The provision applies to information obtained by financial institutions in the course of business.[20] If on the basis of such information a person knows or suspects or has reasonable grounds for knowing or suspecting that another person is engaged in money laundering s/he should make a disclosure by filing a SAR, as soon as it is reasonably practicable to do so.[21] Thus the offense includes negligence-based liability. In other words, liability for breach of

[20] Proceeds of Crime Act, 2002, § 330(3) (U.K.), *available at* http://www.legislation.gov.uk/UKpga/2002/29/pdfs/UKpga_20020029_en.pdf [hereinafter POCA].

[21] *Id.* at §§ 330(2), 330(4). This implements Article 22(1)(a) of the Third Money Laundering Directive, which contains the same wording.

Section 330 may arise not only where a person knows or suspects and does not file a SAR, but also where a person should have known or suspected, as there were reasonable grounds to do so.[22] This introduces an objective test of liability. In order for the obligation to arise, the person must be able to identify the whereabouts of the person or laundered money or s/he must believe, or it is reasonable to expect him/her to believe, that the information may assist in identifying the person or the laundered property.[23]

The failure to report an offense is known as a secondary money laundering offense. In certain circumstances, where it carries out a transaction for a customer in spite of the fact that it suspects money laundering, a financial institution may also be liable for the primary money laundering offenses laid down in POCA, Sections 327-329, in particular Section 328—entering into or becoming concerned in an arrangement which one knows or suspects facilitates (by whatever means) the acquisition, retention, use, or control of criminal property by or on behalf of another person. In order to avoid such liability, consent to the transaction must first be obtained under Section 335. In order to obtain such consent the bank must make a disclosure by filing a "consent SAR."[24] The penalties for acting without consent are potentially very serious, if it is proven that the act constitutes a primary money laundering offense.[25]

So what are the implications of these reporting obligations? Starting first with the implications for the regulator, a stringent

---

[22] *Id.* at § 330(2).

[23] *Id.* at § 330(3)(a).

[24] Having made such disclosure, in order to carry out the transaction for its customer the relevant person must either receive explicit consent, or wait for the expiration of the notice period, *id.* at § 335(3), or, where consent is refused during the notice period, the expiration of the moratorium. *Id.* at § 335(4). The notice period is 7 working days, *id.* at § 335(5), and the moratorium period is 31 days. *Id.* at § 335(6). If no consent is received and either the notice or the moratorium period (if applicable) has not passed, the relevant person can do nothing. If it acts, it may be liable for a primary money laundering offense, as provided by Section 334(1). *See R. v. Serious Organised Crime Agency*, [2007] EWCA (Civ) 406, [51]-[52], [2008] 1 All E.R. 465 (Eng.).

[25] *See* POCA § 334.

requirement with draconian sanctions as provided by U.K. law typically results in large volumes of SARs, which can only be useful to law enforcement if they are organized in and accessed by end-users through a central database. In its early years the U.K. SARs system experienced substantial backlog problems because reports were submitted on paper and then manually inputted into a database by the staff of the then National Criminal Intelligence Service.[26] Law Enforcement Agencies (LEAs)—the end-users of the reports—had no access to the database, so SARs had to be distributed to the end-users within whose jurisdiction they appeared to fall.[27] In order to address these problems, the system was reformed, so that the vast majority of reports began to be submitted electronically,[28] and end-users were given direct access to the ELMER database of reports in 2006. As a result SARs that do not produce "hits" when database searches are undertaken will not usually be followed up on or used in investigations. Because LEAs with scant resources have to prioritize their work, the filing of SARs relating to money-laundering transactions where the predicate offense is a petty crime can therefore be a waste of time and resources for the reporter, unless the SARs in question supplement already existing intelligence. Furthermore, the fact that so many end-users have access to the entire database, which is in effect a database of suspects, can have important implications for individual right to privacy and the confidentiality of personal information.[29]

---

[26] *See* KPMG, REVIEW OF REGIME FOR HANDLING SUSPICIOUS ACTIVITY REPORTS: REPORT OF RECOMMENDATIONS 41-42 (2003).

[27] Matthew H. Fleming, *UK Law Enforcement Agency Use and Management of Suspicious Activity Reports: Towards Determining the Value of the Regime* 27-38 (Univ. College London, 2005), *available at* http://www.ucl.ac.uk/scs/downloads/research-reports/fleming-LEA-SARS.

[28] SERIOUS ORGANISED CRIME AGENCY [SOCA], SUSPICIOUS ACTIVITY REPORTS REGIME ANNUAL REPORT 2011 10 (2011) [hereinafter SOCA ANNUAL REPORT].

[29] *See* EUROPEAN UNION COMM., HOUSE OF LORDS, MONEY LAUNDERING AND THE FINANCING OF TERRORISM VOLUME I: REPORT (2009), *available at* http://www.coe.int/t/dghl/monitoring/moneyval/activities/UK_Parlrep.pdf,
where the Committee observed that "ELMER is in effect a database of suspects," *id.* at 49, containing a large and ever-increasing number of entries, *id.* at 48-49, which can be accessed directly by LEAs not only for purposes related

From the point of view of financial institutions that have the obligation to file reports, compliance with reporting requirements is resource-intensive, in some cases requiring the setting up of automated systems for the identification of unusual activity, and in all cases requiring staff training and man-hours.[30] These costs may have to be passed on to consumers in the form of increased service fees and charges, which may reduce the service's accessibility. Where the necessary resources are simply not available, much suspicious activity may remain unidentified and therefore unreported. It is also important to note that the objective test of *mens rea* coupled with criminal sanctions for breach of reporting requirements gives rise to a certain amount of defensive reporting, i.e., the filing of reports even if the reporter does not believe them to be of any use to law enforcement, which is in effect a waste of resources.[31] At the same time the objective test will not necessarily deter service providers who are complicit with their clients in

---

to serious organized crime but also for other purposes such as "ensuring compliance with tax obligations" and investigating "housing benefit fraud." *Id.* at 49. It also found it noteworthy that "[o]n receipt of a SAR no steps are taken to confirm whether or not the suspicion on which it was based is well founded," *id.*, and that SARs are only automatically deleted ten years following receipt (except for SARs that have been amended or updated, in which case deletion is postponed for six years). *Id.* According to the 2011 SAR Annual Report there are currently 78 end users with direct access to ELMER. *See* SOCA ANNUAL REPORT, *supra* note 28, at 53. However the concerns of the House of Lords Committee have been taken on board and some changes have been implemented. All SARs older than six years will be deleted from ELMER, *id.* at 35, and access by non-police end-users will be subject to compliance with Criteria for Direct Access to Suspicious Activity Reports. *Id.* at 34.

[30] *See* Fred Hobson, *Introduction: Banks and Money Laundering*, *in* BANKS AND FINANCIAL CRIME: THE INTERNATIONAL LAW OF TAINTED MONEY 3, 10 (William Blair & Richard Brent eds., 2008). *See also* Timon Molloy, *Software for Suspicion – One Institution's Experience*, MONEY LAUNDERING BULL., Feb. 2005, at 10-11; Timon Molloy, *The Needle Hunters*, MONEY LAUNDERING BULL., Oct. 2004, at 3-4.

[31] *See* KPMG, *supra* note 26, at 34; Stephen Lander, SOCA, REVIEW OF THE SUSPICIOUS ACTIVITY REPORT REGIME: THE SARS REVIEW 16-17 (2006); FIN. SERVS. AUTHORITY, REVIEW OF PRIVATE BANKS' ANTI-MONEY LAUNDERING SYSTEMS AND CONTROLS 26 (2007), *available at* http://www.fsa.gov.uk/pubs/other/money_laundering/systems.pdf; SOCA, SUSPICIOUS ACTIVITY REPORTS REGIME ANNUAL REPORT 2010 14-15 (2010).

hiding instances of money laundering. A good illustration may be found in the United Kingdom case of *R. v. Swan*[32] where there was ample evidence that both defendants should have been aware that their facilities and services (safe deposit boxes and a bureau de change) were being used for purposes which were not above board. Swan was recorded on tape giving advice to undercover officers on how to launder money through the bureau de change without giving rise to the need for her to report[33] and how to hire a safe deposit box anonymously.[34] Woolf had on occasion found illegal items such as false passports and firearms in client safe deposit boxes.[35] Thus the existence of the obligation in and of itself is no guarantee of the usefulness of the reports that find their way to the authorities.

A further problem is that if a consent system, such as the one in the United Kingdom is in place, filing a SAR can disrupt business and alienate clients. Two civil disputes which arose in the United Kingdom between customers and their banks, *Squirrell Ltd. v. National Westminster Bank*[36] and *K. Ltd. v. National Westminster Bank*,[37] provide interesting illustrations of the awkward situations that may arise as financial institutions seek to operate in the midst of impossible conflicts between their duty to act in accordance with the customer's mandate and their duty to abstain from carrying out suspicious transactions for the customer until consent is obtained. Where a customer is attempting to effect a money transfer, and especially in cases such as these involving the transfer of substantial amounts of money between businesses in different jurisdictions, the delay in effecting the transfers while a financial institution awaits consent from the authorities will have an impact not merely on the relationship between the financial institution and its customer but also on that between the parties to the business transaction (failure to make payment would put a business in breach of its contract with its counterparty). While the financial

---

[32] [2011] EWCA (Crim) 2275 (Eng.).
[33] *Id.* at [3].
[34] *Id.* at [4].
[35] *Id.* at [7].
[36] [2005] EWHC (Ch) 664, [2006] 1 W.L.R. 637 (Eng.).
[37] [2006] EWCA (Civ) 1039, [2007] 1 W.L.R. 311 (Eng.).

institution may not carry out its customer's mandate (and indeed the court held in the above cases that when a conflict arises between a financial institution's duties to its customer and its duties under the criminal law, the latter should prevail), neither may it explain to its customer the reason why, as, if it does, it may find itself in breach of the tipping-off provisions in POCA[38] which implement FATF Recommendation 21(b).[39] While the reporting institution is protected, the customer is left, for all intents and purposes, without a remedy, though the courts have shown some willingness to hold SOCA accountable where it acts outside its powers in withholding consent.[40] Any suspicion will suffice to trigger the financial institution's obligation to report—the suspicion does not have to be reasonable.[41]

III. PROBLEMS WITH IMPLEMENTING A U.K.-STYLE SAR REGIME IN A DEVELOPING COUNTRY

It is not hard to envisage the problems that are likely to arise in attempting to set up a U.K.-style SAR regime applicable to mobile money service providers in a developing country. First of all, in a developing country the application of simplified due diligence will be necessary in many cases in order to achieve financial inclusion, but where simplified due diligence is applied, it is not usually possible to obtain a full client profile. As a result, identification of

---

[38] POCA § 333.

[39] This provides: "Financial institutions, their directors, officers and employees should be . . . prohibited by law from disclosing ('tipping-off') the fact that a suspicious transaction report (STR) or related information is being filed with the FIU." FATF RECOMMENDATIONS, *supra* note 1, at 19.

[40] *R. v. Serious Organised Crime Agency*, [2007] EWCA (Civ) 465.

[41] "Suspicion" is defined in *K. Ltd. v. Nat'l Westminster Bank*, [2006] EWCA (Civ) 1039, [16] as "a possibility, which is more than fanciful, that the relevant facts exist." In the same case it was held that the existence of suspicion was a subjective fact and that there was no legal requirement that there should be reasonable grounds for the suspicion. *Id.* at [21]. In *Ahmad v. HM Advocate*, [2009] HCJAC 60 [30]; (2009) SCL 1093, 1108 (Scot.) it was held that "There is nothing in the language of s 330(2) which states or requires that money laundering is in fact taking place. It is plain that the obligation thereunder can arise if a person suspects or has reasonable cause for suspecting that it is."

suspicious activity will be harder, because the service provider will not always be aware of the client's background and what constitutes unusual activity for the client. In addition, the ability to file meaningful (and therefore useful) reports will be reduced, for example because the client used an alias or because the reason for suspicion is not included or is not sufficiently clear to assist in gathering intelligence for an investigation.[42]

Another problem is that, as far as reporting obligations are concerned, under FATF standards no risk-based approach applies: all suspicions must be reported.[43] Thus reports must be made also with respect to suspicious transactions that are low-value and high volume, i.e., transactions of the type usually carried out using mobile money services. Service providers will need to train staff and devote resources to make these reports in spite of the fact that individual transactions do not present a significant profit margin. This may mean that, depending on the circumstances, certain types of customer may have to be excluded altogether. Furthermore, the authorities will rarely have the resources to justify the investigation of such alleged instances of money laundering,[44] at least not unless the number and pattern of linked transactions indicates a potentially serious problem. It is submitted that any attempt to apply a consent regime to this type of transaction would be ill-advised and likely to fail, both because the timely identification of suspicious and unusual activity is problematic for the abovementioned reasons, and because authorities are unlikely to be able to respond to requests for consent with a promptness that would allow the transaction to be carried out smoothly. Even if a

---

[42] *See* Louis de Koker, *Aligning Anti-Money Laundering, Combating of Financing Terror and Financial Inclusion: Questions to Consider When FATF Standards are Clarified*, 18 J. FIN. CRIME 361, 377 (2011).

[43] *See* FATF RECOMMENDATIONS, *supra* note 1, at 79: "All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction." *See also* FATF, GUIDANCE ON THE RISK-BASED APPROACH TO COMBATING MONEY LAUNDERING AND TERRORIST FINANCING: HIGH LEVEL PRINCIPLES AND PROCEDURES 27 (2007), *available at* http://www.fatf-gafi.org/media/fatf/documents/reports/High%20Level%20Principles%20and%20Procedures.pdf [hereinafter FATF 2007 GUIDANCE]; FATF 2011 GUIDANCE, *supra* note 3, at 40-41.

[44] *See* de Koker, *supra* note 42, at 377.

consent system is correctly implemented, it is likely that customers will abandon mobile money services in favor of more efficient informal payment methods.

A final potential issue involves evaluations of the system that may be carried out by other countries or external entities such as the FATF. In the past the FATF has criticized certain countries for the low volumes of SARs being filed, a prime example being Switzerland in 2005.[45] If the same approach were applied in a developing country, SAR systems may be geared by the regulatory agencies responsible for them to generate defensive and over-reporting in order to improve the country's statistics. An undesired effect could be the establishment of (informal) SARs targets and, potentially, artificial filings by reporters in order to reach an (informal) "quota." This of course would lead to a further waste of authorities' resources.

CONCLUSION

The above analysis leads to a few important conclusions. It is extremely difficult to construct an efficient and effective SAR system. Even in advanced economies like the United Kingdom, where a SAR system has been in operation for a considerable period of time, there are still open questions as to the system's effectiveness.[46] The inclusion of financial activity taking place by means of new payment methods such as mobile money within the ambit of a SAR system will require that system to be adapted, especially where a new type of provider, (i.e., a telecommunications company rather than a traditional financial

---

[45] "The number of reports of suspicions filed with MROS seems low given the scale of the Swiss financial market and the activity that is carried out there." FATF, THIRD MUTUAL EVALUATION REPORT ON ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM: SWITZERLAND 7 (2005), *available at* http://www.fatf-gafi.org/media/fatf/documents/reports/mer/mer%20switzerland%20resume%20english.pdf.

[46] *See* Miriam Goldby, *Anti-Money Laundering Reporting Requirements Imposed by English Law: Measuring Effectiveness and Gauging the Need for Reform* 1 J. BUS. L. (forthcoming Spring 2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2012448.

institution) with different types of internal monitoring and record-keeping processes, is providing the service. It is submitted that the FATF reporting requirements do not differentiate sufficiently among different circumstances and are not appropriately tested for unwanted "side-effects" such as wasteful defensive reporting or the shunning by consumers of regulated services in favor of informal ones, which may be cheaper and more efficient due to the absence of regulatory burdens.

In order to assist developing countries in designing a SAR system that will achieve some measure of financial integrity in this type of situation, FATF must do its utmost to move away from a one-size-fits-all approach and identify the most effective means to monitor mobile money transactions in developing countries. This entails the possibility of doing away with a traditional SAR system altogether and considering alternatives which allow countries to tailor their approach to financial integrity to their own environments. While the SAR system set up in the United Kingdom may be suitable for the jurisdiction in which it operates (and even this is as yet an open question),[47] the application of suspicious activity reporting requirements in the same way in developing countries would be unsuitable. In particular, red tape in submitting reports should be kept to a minimum and, pending development of an appropriate and reliable infrastructure for web-based communications, reports in all forms should be acceptable. Depending on the circumstances, compliance with CDD and record-keeping requirements[48] may preclude the need for SARs except for actual and strong suspicions. Instead a service provider's records on a person officially under investigation could be made accessible to LEAs. As we have seen in the U.K. system SARs are put on a database which LEAs consult with search terms, usually for known nominals, and do not usually of themselves form the starting point of an investigation. This being the case, a similar effect could be achieved if LEAs were allowed, under certain conditions, to conduct searches of the records kept by service providers, which would preclude the need to file SARs.

---

[47] *See id.*

[48] For a discussion of record-keeping requirements applicable to mobile money service providers, see FATF 2011 GUIDANCE, *supra* note 3, at 40.

When drafting provisions granting these powers, however, it is important to build in safeguards against potential abuses by governmental agencies, which may have the effect of discouraging widespread use of mobile money services.[49]

Finally, if a consent regime is put in place, it should only apply to high-risk transactions, for example transactions over a certain threshold value and/or transactions which the reporter knows or has reason to believe are linked to a serious predicate crime such as serious theft; fraud; corruption; the trafficking of weapons, drugs, or people; or terrorism offenses.

Much research remains to be done into the effectiveness of SAR regimes and this research should be undertaken before attempts are made to make these regimes applicable to mobile money service providers in developing countries. A one-size-fits-all approach is likely to result in many unintended effects which will at best slow down the dissemination of this type of financial service in the areas that need it most and at worst lead to its outright rejection by intended users.

[49] *See* Louis de Koker & Nicola Jentzsch, Financial Inclusion and Financial Integrity: Aligned Incentives? (July 2011) (unpublished conference paper, Univ. of Münster), *available at* http://dro.deakin.edu.au/view/DU:30041719.