Introduction

There has been an increase use of mobile money involving retail users and financial institutions (Scobey-Thal, 2015). In 2015, the GSMA (an organization that represent the interests of mobile operators worldwide) states that there are more than 411 million mobile money accounts around the world. Furthermore, mobile money accounts have penetrated 85% of countries, often where a majority of the population do not have access to a formal financial institution (GSMA, 2015). Cisco Systems Inc. (2017) estimates that by 2021, more people will have access to mobile phones than there will be access to running water. Given the enormous growth in the mobile market, it is internationally recognised that this penetration should be capitalised on in the form of financial inclusion. However, with such benefits, come new challenges and the success of mobile money depends on the industry’s ability to adjust to a rapidly changing financial landscape (GSMA, 2015).

A combination of exponential mobile growth and emerging financial services creates new opportunities for criminals to exploit vulnerabilities in the system. Although there have not been many cases of mobile money laundering, it is important to consider the potential to commit fraudulent activities. Technology advancements continue to change the very architecture of financial services by becoming complex value chain networks. As these services continue to diversify, there is an urgent need for more adaptive and fluid regulation (Braithwaite, 2013) to identify, address and mitigate threats as they arise (Lokanan, 2017). As a result,
anti-money laundering (AML) and counter terrorist financing (CTF) regimes remain operationally fluid, whilst accrediting global financial integrity. This concern lays the foundation for our research question: What can be done to mitigate anti-money laundering and counter-terrorist financing threats posed by mobile money? In this regard, the purpose of the paper is to explore the various characteristics of mobile money that presents a threat to anti-money laundering and counter terrorist financing regimes.

The rest of the paper proceeds as follows. First, we conduct a literature review on mobile money. Second, we described the methodology used to identify the main themes in the study. Third, we conducted an analysis of the themes identified in relations to the three stages of money laundering and law enforcement. In this section, we assess the varying threats associated with the mobile money. Finally, we conclude the paper with recommendations on how the threats associated with mobile money can be mitigated.

**Mobile Money as an Umbrella Concept**

Mobile payment is an umbrella term that encompasses mobile money, mobile banking, mobile wallets, mobile money remittance and e-money. Mobile money can be used as a form of ‘mobile wallet’. This allows digital repository of electronic money, which facilitates peer-to-peer (P2P) transactions, enabled through mobile-to-mobile (M2M) regardless of the handset used (De Albuquerque, Diniz, & Cernev, 2016). Donner & Tellez (2008) collectively refers to the terms of m-payments, m-transfers, m-banking and m-finance as a set of applications enabled through mobile handsets to store value in an account linked to their handsets, manipulate their bank accounts, transfer funds, and
access insurance products and credit. Mobile devices connect customers to payment systems that operate under financial regulation. With this, mobile money is swiftly becoming a preferred alternative to cash, check or credit cards as the devices can also enable consumers to purchase a wide variety of goods and services. Mobile money can also be differentiated with other means of electronic payment methods including debit cards and credit cards due to its ability to replicate the characteristics of traditional money (cash), such as liquidity, acceptability and anonymity (De Albuquerque et al., 2016).

**The Alleged Threat of Mobile Money**

Considering the scale of worldwide mobile ownership and increasing m-payment usage, it is important to consider the potential avenues in which criminals could commit money laundering activities and create systemic risks. The threats of mobile money are enabled through the structure of global information and communication networks and the way that they operate. These networks create opportunities in which cyber launderers seek to exploit by means of anonymity, rapidity, ease of use and the ability to operate in different jurisdictions without being physically present. This approach reduces the risks of being detected and prosecuted and increases elusiveness, all of which is enabled through m-payment transfer systems (Filipkowski, 2008; Tropina, 2014). In so doing, they are able to bypassed the traditional ML vulnerabilities of transporting large sums of cash, which could be detected through algorithmic mechanisms especially across jurisdictions (Williams, 2013). When funds is loaded to a mobile device, it is not subject to initial investigation, unless there are red flags of potential money laundering activities.
One major concerning factor associated with mobile money is micro-structuring, more commonly referred to as ‘smurfing’ or in the case of mobile money ‘digital smurfing’. This can occur if multiple third parties (runners/smurfs) or third party accounts are under instruction by a professional money launderer to transfer illicit funds, which has been split into smaller values conforming to legal reporting limit. The aim is to evade AML reporting requirements and thus reducing fraud detection creating the risk of elusiveness while adding complexity to the money trail (Zhdanova, Repp, Ricke, Gaber, & Hemery, 2014). Other advantages of using digital smurfing include the fast convergence from cash to digital value. This is a highly prevalent process in which organised criminal networks benefit from and is common throughout the United States (Cassara, 2016).

Law enforcement will be further challenged by means of cross border fraudulent activities, if crimes are committed in a host country and remitted to multiple countries. Both or for that matter, multiple jurisdictions would need to approve the investigation processes. Remittances can be sent to jurisdictions, which criminals know lack the capacity and competency of tracking organised crime; this is common in developing countries. Further complexities arise in the form of insubstantial physical evidence. If the remitter or recipient destroys the mobile device it may be impossible to locate the audit trail. Both of these are factors that make enforcement a difficult proposition.

In some cases, mobiles’ connections are enabled through prepaid services, of which some mobile network operators (MNO) do not require prior identification or verification to enable telecommunication access and creates
anonymity risks. An equally inherent threat can be created if false identification is provided allowing persons to establish a mobile money service account (Cassara, 2012). This is especially hard to detect unless proper systems and controls are in place to prevent such occurrences when there is no face-to-face contact to conduct customer’s due diligence measures (Walker, 2017). Such threats can further materialise if there is lacking regulatory and supervisory oversight to ensure mobile money service providers are enforcing AML compliance measures throughout their vulnerable business lines.

**Threat of Mobile Money Stage 1 – Placement/ Loading**

The first stage of the money laundering process is placement. Placement is where funds are placed into the formal financial system. Traditionally, placement involves the physical movement of money to incorporate distance between the illicit funds origin and to avoid confiscation (Dumitrache & Modiga, 2011). However, in the virtual world, this stage can be overcome due to the loaded value already existing in electronic form (Filipkowski, 2008; Dumitrache & Modiga, 2011). Placement could potentially be loaded into an inadequately regulated financial institution or MNO creating the threat of oversight (Suárez, 2016) as they are subject to less stringent identification screening measures. This also presents the risk of customers’ anonymity because of multiple accounts registration in an attempt to avoid detection (Dumitrache & Modiga, 2011). Additionally, illicit funds can be split into smaller values below the minimum reporting limit thereby avoiding ‘red flags’ and create the risk of elusiveness (Filipkowski, 2008).
Threat of Mobile Money Stage 2 – Layering/ Transferring

The second stage is the movement from one value location to another to complicate the money trail or ‘original origin’. Mobile value can be transferred from one account to another, or credited to a mobile money account, and then forwarded onto a money service business (MSB) or other financial institution in the host country, or worse, still transferred abroad or even an offshore haven (Cassara, 2016). The use of extensive money trails are common aims by money launderers. It is a technique that can be done rapidly, including several jurisdictions; together, these work to complicate law enforcement measures (Filipkowski, 2008). According to Dumitrache and Modiga (2011), due to the speed, volume and ability to perform international remittances, it is unlikely that law enforcement will investigate at this stage.

Threat of Mobile Money Stage 3 – Integration/ Withdrawing

The final stage has the sole purpose of making the illicit funds appear legitimately obtained. This is done through the purchase of goods or services and where the laundered funds are integrated into the financial economy. In relation to mobile money, this could be a continuation of the ‘layering’ stage, or potentially using this to integrate the illicit funds into the financial system though the purchase of goods. The rapidity of remitted funds, combined with anonymity at the initial loading stage to further fund criminal activity is considered a serious threat to AML and financial integrity (Solin & Zerzan, 2010).
Methodology

For the purpose of this study, a thematic analysis was performed to gather data. Thematic analysis is a type of qualitative descriptive approach used to “analyse classifications and present themes (patterns) that relate to the data” (Alhojailan, 2012, p. 40). It allows the researcher to explore the significance of an idea, while developing an understanding of the issue through contextualising results (Stirling, 2001, p. 387).

The sources of the literature examined throughout this paper were obtained from academic books, credible author publications and mainly scholarly journals. The bulk and scope of these publications ranged between 2008 and 2017, and were used to enforce the credibility of the findings. This approach also formed the premise for timely thematic analysis to be conducted and draw conclusions from recurring key words and phrases. The literature was then scored by repeated use and translated into key recurring themes. This resulted in four main categories relative to the data and information examined. Table 1 below shows the categories of the data. The asterisks correspond to the level of risk with one asterisk being low risk, two asterisks being medium risk and three asterisks being high risk.

Table 1: A Comparison between Cash and Mobile Money Characteristics

<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>Cash</th>
<th>Mobile Money</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Anonymity</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Untraceable source</td>
<td>***</td>
<td>Pre-paid phones can have no registration requirements</td>
</tr>
<tr>
<td>No individual reference code of value transaction</td>
<td></td>
<td>Linked to account/subscription/mobile number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Open numerous accounts to digital smurfs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Absent or inefficient systems to red flag suspicious names</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Limited face-to-face contact</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Transaction values recorded and monitored</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Cash</th>
<th>Mobile Money</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Consideration</strong></td>
<td><strong>Risk Rating</strong></td>
<td><strong>Consideration</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Elusiveness</td>
<td>Facilitates continuous monitoring</td>
<td>At least - minimum KYC requirements</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>No monitoring of monetary flow</td>
<td>*** Smurf can place value into numerous accounts</td>
<td>**</td>
</tr>
<tr>
<td>Undetectable unless declared</td>
<td>Traceability of payments and withdrawals</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Difficulty in compiling an aggregate of multiple transactions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Transaction details (value, time, location)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sending values under the regulatory limit to avoid flagging detection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Digital footprints</td>
<td></td>
</tr>
<tr>
<td></td>
<td>At least - basic sender and receiver details</td>
<td></td>
</tr>
<tr>
<td>Rapidity</td>
<td>Typically slow movement (dependent on transportation method)</td>
<td></td>
</tr>
<tr>
<td>Immovable unless physical</td>
<td>* Ability to perform multiple payments, move between accounts and value withdrawn rapidly</td>
<td>***</td>
</tr>
<tr>
<td></td>
<td>Ability to load/ transfer from alternative sources</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Effortless</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Real time transactions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Local, regional and international payments</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Poor systems and monitoring – if values are below the flagging limit, unlikely transaction is placed on hold</td>
<td></td>
</tr>
<tr>
<td>Lack of Oversight</td>
<td>No regulation monitoring unless declared (Tax, border control)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>*** Supervision and regulation varies on service provider and geographical location</td>
<td>**</td>
</tr>
<tr>
<td></td>
<td>Can vary from: none, inadequate due to lower standards nationally/ internationally of financial institutions(FI), adequately/ in line with standards nationally and/or internationally</td>
<td></td>
</tr>
</tbody>
</table>
Analysis

For the purpose of the following discussion, the categories identified as the main risk factors to anti-money laundering activities are anonymity, elusiveness, rapidity and lack of oversight. Each one of these risk factors will be explained followed by an analysis relating them back to the threat associated with the three money laundering stages - loading, transferring and withdrawing.

Risk Factors Associated with Anti-Money Laundering and Counter Terrorist Financing

The following four risk factors identified throughout the literature have been developed from GSMA’s mobile money risk assessment methodology (Solin & Zerzan, 2010). The first three risks factors are inherently related to the business model; lack of oversight creates condition that increases the likelihood of the emerging three risks (Raphael, 2016). These are in fact typical risk factors that AML seeks to mitigate, and therefore this will form the basis of the analysis. Table 1 allows for a characteristic comparison against traditional cash and mobile money transfers. Against these risk factors, the risk ratings are marked with asterisks to indicate a high, medium and low risk respectively.

Anonymity

In the context of mobile usage, Gow and Parisi (2009) argue that it may be impossible in practical terms to remain truly anonymous in the case of mobile usage. However, in this instance, it is assumed that due to relaxed Know Your Customer (KYC) and Customer Due Diligence (CDD) requirements, the individual using a mobile money service has the ability to uphold some form of
anonymity through false identification or not disclosing their identity to the MSB. In the case where identification is provided, but there are weak or none existent verification processes, the individual can commit identity fraud usually due to two prevailing reasons. First, in cases where there are non-face-to-face transaction, some jurisdictions may offer financial services and benefits to facilitate inclusion. Second, the jurisdiction has a weak verification structure (Chatain et al., 2011). These are usually most prevalent in developing economies and not uncommon in relation to mobile money (de Koker, 2011).

Chatain et al., (2008) also identified presenting counterfeit documentation as an integral risk to mobile financial services. If false identification is presented when purchasing a mobile phone, subsequent usage from potential criminals using the phone may be unidentifiable. Furthermore, there are concerns that mobiles linked to mobile money accounts may be handed over to criminals or the phone may also be stolen in the hope that transactions may go unmonitored and facilitate fraudulent activities (Chatain et al., 2008). What is evident from the discussion so far is that mobile money does present the opportunity to perform transactions anonymously; this risk can only be mitigated through enhanced CDD procedures (Solin & Zerzan, 2010).

In terms of assessing the anonymity threat, Gow and Parisi (2009) argue that mobile money due to it being in digital form, are able to record all activities through digital footprints. This is certainly a characteristic which is much more favourable than cash transactions as it is untraceable, and subsequently poses a lower threat of getting caught. The potential threat of unassigned identification to prepaid phones can indeed create anonymity. This threat can be further
materialised at the withdrawing ML stage since value can be sent to an unidentified phone, where the money can be withdrawn from an agent, who then get rid of the mobile and thereby rendering it near impossible to track the individual. As for false identification, this is certainly a potential threat, especially when service providers do not have proper verification channels to cross verify identities and criminal databases. This is a particular threat at all three ML stages. Since known criminals or terrorists cannot be identified easily, rendering the provider as a potential safe zone can further attract criminals to exploit the weaknesses in the transfer system. In cases where false identification is provided by multiple smurfs to establish an account, they become serious threats at the loading stage as red flags are not generated. This conduct is only considered a medium threat if there are no or insufficient identification and verification procedures, crucial for profile building to stop previously identified fraudsters.

**Elusiveness**

Elusiveness relates to the ability of the individual to disguise mobile transaction totals, origins and destinations (Chatain et al., 2009). This is an inherent risk relating to the general characteristics of fraud with the aim of evading detection. The theory is that m-payments facilitate hundreds of small value transactions relatively easily after splitting the total value also known as smurfing. In doing so, the transaction value becomes low enough to comply with legal reporting limit in most jurisdictions, evades detection, and used to fund illegal and terrorist activities. This is particularly problematic for law enforcement agencies as they need to uncover the money trails, which would be highly difficult without some invasion of privacy (Ashta, 2017). Law enforcement
departments in the past have acted on this concern, which resulted in increase
detection of smurfing activities (Chatain et al., 2011). To offset the increased
detection, criminal syndicates have further lowered the values in an attempt to
evade detection (Filipkowski, 2008; Tropina, 2014).

The inherent risks outlined above do provide criminals with their desired
ability to remain elusive. Mobile money certainly does add heightened
complexities for law enforcement prosecution. A much more serious risk lies with
digital smurfing. Originally cash would have had to be physically moved, which
is precarious in the sense that the element of detection is inherently higher than
carrying a mobile device that is loaded with funds. Initial suspicions would not be
raised at a person carrying a mobile phone thereby remaining elusive. Organised
criminal networks can employ numerous smurfs, which if they are caught, the
professional money launderer can evade prosecution and adds to the complexities
to infiltrate money laundering networks. This being said, due to mobile
transactions passing through the provider based networks, there is the ability to
monitor transactions while obtaining telephone numbers, value amount, time, date
and possibly location. Elusiveness is considered a medium threat because there is
a lack of identification and verification. It is consistent with the ML loading stage
and relates to the ability to load funds into multiple accounts performed by
smurfs.

**Rapidity**

An undesirable consequence of legitimate users benefitting from the
rapidity of mobile transactions is an inherent threat to anti-money laundering
legislations. Rapidity further substantiates the initial three threats as transactions
are completed in real time, which could involve transactions crossing multiple jurisdictions and further complicates the law enforcement process (Filipkowski, 2008). Due to its speed of transaction, if the value is remitted and confirms to legal reporting limits, and does not generate ‘red flags’, the illicit funds could be received and withdrawn and the account could be closed before AML compliance officers, regulatory bodies and law enforcement has time to intervene (Ashta, 2017). In cases where the transaction is operated through an organised criminal network, the withdraw funds could be further passed onto smurfs to add further complexities to the money trail. Criminals utilise this element as it overcomes many of the obstacles evident through traditional money laundering operations. The speed also takes layering to new levels over the traditional methods, which would require face-to-face interaction at a financial institution (Chatain et al., 2011).

Rapidity is certainly the most significant threat when compared with cash as value can be remitted, in real time, relatively easy, efficiently and without the need of physical movement. The ability to remit value on an intentional basis takes money laundering possibilities global. Mobile money users adapt to this platform due to its obvious benefits of being able to remit value rapidly. If such systems that were used to uphold AML requirements prevented the transaction to be complete, it will be counterproductive to legitimate user experience. If users feel that they are being monitored, it may inadvertently drive users to alternative payment methods, as privacy and potential exploitation are considered significant causes for concern in developing countries.
Rapidity is only to be considered the highest risk of the four if there are no or insufficient AML systems and controls in place to detect and prevent money laundering activities in real time (Walker, 2017). In instances where this is not the case, then the company is likely to be further targeted due to its ML/TF inefficiencies. At the loading stage, rapidity is a threat in terms of the ability to deposit illicit funds quickly, and as such, the placement process is initiated making its way into the electronic system. Rapidity is also considered a serious threat at the transferring (layering) stage. After mass transferring, the funds can then be withdrawn equally as quickly. The threat of rapidity throughout all three stages could be further multiplied with the added factor of smurfs.

**Lack of Oversight**

A lack of oversight does not constitute an inherent risk on its own, but it does further add and intensify the initial three inherent risks (Chatain, Hernández-Coss, Borowik, & Zerzan, 2008) with the potential to cause systemic risk. This lack of oversight has originated due to unclear boundaries in laws, regulations and the establishment of a clearly defined overseer. As globalisation drives innovations such as mobile money, for many countries m-money has not been defined in AML/CTF regulations. This is because regulations were not created with m-money in mind as a financial platform, which then leaves countries attempting to bridge the gap with inadequate laws and regulations that would normally apply to the formal banking sector. For example, telecommunication companies providing financial services can inherently create the risk of lack of oversight because financial services are not their primary business focus (Chatain *et al.*, 2011); as a result, they lack the financial intricacies
to effectively oversee their business lines when they are exposed to potential risks. Similarly, when the service is enabled through the bank-led model, confusion arises as to who should take the lead in the supervisory role (Stephens, 2012). This ambiguity needs to be clearly defined and is often not the case.

In terms of assessing the risk derived from lack of oversight, there are numerous elements that add to its complexity. Oversight risk often originates in countries, which are not fully up to speed with financial regulation. Usually because there is insufficient understanding of how mobile money operates, and the ability to identify vulnerabilities in the system, money launderers see this as an opportunity to exploit an inefficient and under-policed apparatus (Power, 2013). This being said, cash economies pose a greater risk than mobile money through general lack of oversight. In order for the service provider to enable m-payment services, it can either be overseen by the bank if a partnership is established or through the registration as a licence holder in which the relevant jurisdictional regulator is assigned to oversee activities. Lawmakers and regulators need to fine-tune their approach to identify the areas in which intervention is required to uphold financial integrity and create a favourable regulatory environment for mobile money and financial inclusion.

**Mitigating the Four Anti-Money Laundering Risk Factors**

After the initial indicators were assigned to the four key risk factors, the table below allows for the risk rating to be compared pre and post implementation of AML/CTF systems and controls. Table 2 shows the visualisation of risk rating before and after, noting that if proper systems, controls and caps are in place, the integrity risk associated with the four categories is severely mitigated to less of a
potential threat than cash transactions. Following Table 2 identification of systems and controls to mitigate the AML/CTF risks, the mitigators are categorised to best address the threats directly and appropriately. The first is a collaboration in which all risks should be addressed, while directly targeting the threat posed by lack of oversight.

**Table 2 A Comparison between Cash and Mobile Money Pre and Post Implementation of Systems and Controls**

<table>
<thead>
<tr>
<th>Risk Factor</th>
<th>Cash</th>
<th>Mobile Money</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Anonymity</strong></td>
<td>***</td>
<td>**</td>
</tr>
<tr>
<td>Risk Rating</td>
<td>Pre-Risk Rating</td>
<td>Implementation of Systems and Controls</td>
</tr>
<tr>
<td><strong>Risk Factor</strong></td>
<td><strong>Cash</strong></td>
<td><strong>Mobile Money</strong></td>
</tr>
<tr>
<td>Anonymity</td>
<td><strong>KYC and KYCC profile building – effective and appropriate systems where face-to-face assessment isn’t available.</strong></td>
<td>Enforce maximum CDD and KYC where possible - after risk assessment.</td>
</tr>
<tr>
<td>Elusiveness</td>
<td>***</td>
<td>** Real-time monitoring – payments, withdrawals, transfers, digital footprints.**</td>
</tr>
<tr>
<td>Rapidity</td>
<td>*</td>
<td>*** Adequate or above adequate systems and monitoring, that does not compromise the speed of legitimate transactions.</td>
</tr>
</tbody>
</table>

1 Table 2 has been adopted from GSMA risk assessment methodology (Solin & Zerzan, 2010)
Real-time monitoring.
Limits on transaction frequency.
Restrictions on identified high risk jurisdictions.

<table>
<thead>
<tr>
<th>Lack of Oversight</th>
<th>***</th>
<th>**</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restriction of value/volume of transactions in specific jurisdictions based on high ML/TF risk association or non-existent/minimal AML laws.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Establishment of independent central compliance system.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ability to tip-off anonymously to relevant Financial Intelligence Unit.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maintain identification and transaction data for minimum of 5 years – Requires jurisdiction risk assessment to determine if a longer retention period is required.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Appropriate Regulation, Supervision and Risk-Based Approach**

It is universally recognised that in order to uphold AML and CTF policies efficiently and effectively, regulators must follow a risk-based approach (Buckley, Greenacre, & Maldy, 2015; FATF, 2013; Solin & Zerzan, 2010). This is simply because a risk-based approach recognises that one solution does not fit all circumstances, and must be tailored to the risk profile for the institution and the nature of business activity. Ideally, the approach should follow a service risk-based approach as opposed to having a provider, a method that is common throughout the world and leads to regulatory overlap.

In order to quantify risks and allocate resources effectively, an institution should conduct risk assessments for its customer base, geographical operations and services. Small institutions reporting to one centralised department can therefore operate effectively with limited inherent risk, while larger organisations may be required to have a multifaceted approach for each line of business reporting to a central or regional compliance function (Axelrod & Ross, 2012). It
is important to recognise here that existing threats evolve and new threats are constantly emerging. The following diagram has been adopted from a risk assessment methodology produced by GSMA. The flow diagram illustrates the procedure of risk assessments as a one-way process. In opposition, risk assessments should follow a continuous non-static cycle to adjust for new and emerging risks (Tropina, 2014) and act as an essential mechanism to facilitate the rapidly evolving mobile money industry. At the heart of the risk assessment, it is fundamentally imperative that the risk assessor has comprehensive knowledge and understanding of the mobile money service in order to effectively mitigate risk (Tropina, 2014). This process will enable an AML framework that is operating at it most optimum, accommodating dynamic changes to their services, customer base and markets.
Figure 1: Five Star Risk-based Approach to Mobile Money Services

It is also unanimously recognised that regulation and supervision must be aligned to the strategy of risk-based assessment outlined above and create a sound and robust AML structure that is tailored to the relative risk introduced by the financial system (Buckley et al., 2015; FATF, 2013). This risk-based focus should proactively involve entities in the process of developing an effective regulatory framework and creates a level playing field within the mobile money industry to be more responsive to new market players and technological innovations (Buckley et al., 2015; FATF, 2013; Tropina, 2014). The opportunity

---

2 Figure 1 is created by the authors and was adapted from GSMA (Solin & Zerzan, 2010).
for voluntary industry engagement in policy development, enables regulation to keep pace with industry developments, ‘fine tuning’ the rules and detangling the bank-led and non-bank-led models (Murray, 2010). Together, these can be beneficial to regulators, market players and end-users as risks are identified in conjunction with appropriate risk mitigation measures. In doing so, AML will be at its most robust at the operative level (Buckley et al., 2015; Solin & Zerzan, 2010; Tropina, 2014).

**Tailored Customer Due Diligence, Know-Your-Customer, Value Limits**

The role of CDD and KYC play a pivotal role in the anti-money laundering regime in the risk-based approach. These measures reduce the anonymity threat through the development of customer profile building that supports transaction monitoring and reduce elusiveness through identifying customer’s financial behaviours (Malady, Buckley, & Arner, 2014). That said, these measures are difficult to implement in the case of mobile money because transactions are being conducted without face-to-face contact to uphold CDD requirements (FATF, 2013; Tropina, 2014).

The general principle for a risk-based approach to AML/CTF measures and supervision is that in cases where higher risks are identified after assessment, enhanced CDD measures are required to mitigate the perceived high risk, whereas in lower risks, it is acceptable to implement simplified CDD measures. In other cases, exemptions from CDD can be applied although this requires exemplary justification and is often not acceptable (FATF, 2013; Malady et al., 2014). Simplified due diligence (SDD) means that identification, verification and monitoring measures can be less formal and less rigorous (FATF, 2012). SDD
can advocate the establishment of hierarchical account capabilities. In instances where KYC has been limited, basic access to accounts can be permitted like mobile wallets with low transaction limits and restricted functions. In order for account restrictions to be lifted, customers must provide more conclusive identity verifications (Chatain et al., 2011; FATF, 2013; Malady et al., 2014). This financial access approach enables the provider to effectively mitigate anonymity threats, while also establishing authenticity for legitimate service uses (Malady et al., 2014). Encompassing this approach will provide a platform, which is not counterproductive to financial inclusion, whereby it can drive consumers to alternative payment methods such as cash, or worse still, further into underground economies to avoid law enforcements (Silva, 2015).

Identification processes should be inherently cross verified following the establishment of client relationships to reduce anonymity (de Koker, 2009; Malady et al., 2014). This can be done relatively easily if appropriate channels for systems and controls to complete identification and verification processes are in place. When the client establishes a relationship with the relevant MNO, regardless of pre-paid or not, anonymity risk can be mitigated with some form of identification requirements to enable access to m-payment services (Chatain et al., 2011; de Koker, 2009; The Wolfsberg Group, 2014). The implementation of these measures would successfully mitigate anonymity and elusiveness risks while also contribute to a more proficient oversight regime (Murray, 2010).

**Technology Enabling Solutions**

Technology should play a more pivotal role in fulfilling the roles of customer due diligence (Abel & MacKay, 2016; Demitracche & Modiga, 2011;
Williams, 2013). The intricacies of mobile technology especially smart phones have the capability to achieve more robust identification and verification processes through tools such as voice and facial recognition, or even fingerprint technology. These methods would be the most effective to reduce anonymity threats by uniquely identifying the individual using m-payment services.

Following the risk assessments of elusiveness and rapidity, smurfing was considered an integral contributor to these risks. Zhdanova et al., (2014) presented a methodology to uncover smurfing fraud chains in mobile money transfer systems. Their system was an extension of Predictive Security Analysis at Runtime (PSA@R), which is a model-based approach for event-driven process analysis that monitors end user behaviour to identify fraudsters. Zhdanova et al., (2014) system simulated 460,000 transactions for 100,000 end users. Their results found 99.81% precision and 90.18% recall rates. This is a prime example of technology innovation playing a pivotal role in protecting AML regimes, while stopping fraud in real-time before the threat can further materialise.

Technology is also fundamental to mitigate elusive and rapidity threats not only by identifying individual fraudsters, but to detect complete fraud chains throughout the mobile money transfer system. A service provider who implements such systems and controls, would be in a position to identify and potentially block mobile numbers in real-time. A limitation of this approach is that in order to prosecute the individuals, the owner of the mobile number must can be found, which is often not the case (Abel & MacKay, 2016; Murray, 2010; Zhdanova et al., 2014). Systems of this nature successfully mitigate anonymity, elusivness, rapidity and systemic risks while contributing to financial integrity.
Technology is overcoming significant business challenges for identification, verification, tracking and monitoring purposes, especially where non-face-to-face transactions occur (de Koker, 2011), while also suppressing criminal activity before it even starts (Dumitrache & Modiga, 2011). Technology lays the foundation for digital transaction tractability, which play crucial roles in achieving AML requirements to monitor, recordkeeping and reporting suspected criminal activity.

**Conclusion**

Mobile money is changing the global financial architecture by bringing benefits to legitimate users. However, as money laundering criminals continue to gravitate towards the weaknesses in the financial system, mobile money provides yet another avenue for criminals to exploit. Given its potential global scale, it is important to identify key ML threats and identify how to mitigate these risks. The use of mobile money has increased exponentially, whilst encouraging robust financial integrity by means of bringing cash dominated economies into the global regulated system. Mobile money allows local and international remittances to be transferred rapidly, benefitting many lives of the financially underserved. Although rapidity is a characteristic in which many legitimate users benefit from, its fluidity is a fundamental threat to AML regimes.

The four risk factors identified allowed for an analysis of mobile money transfer and method to mitigate threats that accompanies its use. The forgoing analysis shows how criminals can exploit vulnerabilities throughout the three money laundering stages. An analysis of the findings shows that the use of cash is considered a higher threat than mobile money prior to implementation of systems.
and controls. This was inherently due to cash having no tractability or movement tracking ability, and in so doing, creates anonymity and elusiveness risks. On the other hand, mobile money consisting in electronic form could be identified through digital footprints. Rapidity was considered the highest risk factor due to transactions occurring in real time, whereas cash had to be physically moved from one location to another. Lastly, lack of oversight was also considered a high threat, which inherently increased the probability of the initial three risks threats.

Overall, the findings show that after the implementation of appropriate systems and controls following the established 5 Star Risk Assessment Cycle, the threats posed by mobile money could be severely mitigated to less of a threat than cash. Risk-based approach should be applied by service provided and not categorised by provider as this was found to add to the complexity of lack of oversight. This approach should be conducted throughout all business lines and periodically reassessed. In doing so, AML will be at its most optimum efficiency and effectively mitigate the four risk factors identified in this paper.
References


