



**USAID**  
FROM THE AMERICAN PEOPLE



# Standards and Practices Report for Electronic and Mobile Payments

**June 2012**

This report was produced for review by the United States Agency for International Development. It was prepared by Deloitte Consulting, LLP under the Global Broadband Innovations Alliance (GBi).

**DISCLAIMER:** The authors' views expressed in this report do not necessarily reflect the views of the United States Agency for International Development of the United States Government or GBi.

# TABLE OF CONTENTS

<b>1. OVERVIEW</b>	<b>1</b>
1.1. OBJECTIVE OF THIS REPORT	2
1.2. PAYMENT TYPES	3
1.3. REGULATORY ENVIRONMENT	5
1.3.1. <i>Government Regulation Impacting Payment Systems</i>	6
1.3.2. <i>Private and Non-Governmental Sector Payments Standards and Policies</i>	7
1.3.3. <i>USAID Funds Disbursement Guidelines</i>	7
<b>2. STAKEHOLDERS</b>	<b>10</b>
2.1. DIRECT STAKEHOLDERS	10
2.2. INDIRECT STAKEHOLDERS	11
<b>3. MATURE PAYMENT METHODS</b>	<b>13</b>
3.1. BACKGROUND AND GOVERNING REGULATION	13
3.1.1. <i>1 – Flow of Funds from USAID Washington to Missions or Implementing Partners</i>	13
3.1.2. <i>2 – Flow of Funds from Missions or Implementing Partners to Sub/Local Contractors</i>	14
3.1.3. <i>3 – Flow of Funds from Implementing Partners to Payment Beneficiaries</i>	14
3.2. PAYMENT METHODS	15
3.2.1. <i>Electronic Funds Transfer / Wire Transfer</i>	15
3.2.2. <i>Cash Payments</i>	19
<b>4. ELECTRONIC AND MOBILE PAYMENTS</b>	<b>23</b>
4.1. ELECTRONIC PAYMENTS: PRE-PAID CARDS	23
4.1.1. <i>Description: Pre-paid Cards</i>	25
4.1.2. <i>Uses, Limitations, Risks, and Mitigants: Pre-paid Cards</i>	25
4.1.3. <i>Regulation: Pre-paid Cards</i>	27
4.2. MOBILE PAYMENTS	30
4.2.1. <i>Description: Mobile Remote Payments</i>	31
4.2.2. <i>Uses, Limitations, Risks, and Mitigants: Mobile Remote Payments</i>	34
4.2.3. <i>Regulation: Mobile Remote Payments</i>	36
4.2.4. <i>Description: Mobile Proximity Payments</i>	36
4.2.5. <i>Uses, Limitations, Risks, and Mitigants: Mobile Proximity Payments</i>	37
4.2.6. <i>Regulation: Mobile Proximity Payments</i>	38
<b>5. RISK ANALYSIS AND MITIGATION</b>	<b>39</b>
5.1. FINANCIAL RISK	40
5.1.1. <i>Cash Payments</i>	41
5.1.2. <i>Electronic Funds Transfer</i>	43
5.1.3. <i>Pre-paid Cards</i>	44
5.1.4. <i>Mobile Payments</i>	45
5.1.5. <i>Relevance to USAID and Implementing Partners</i>	46
5.2. SYSTEMIC RISK	47
5.2.1. <i>Cash Payments</i>	48
5.2.2. <i>Electronic Funds Transfer</i>	49
5.2.3. <i>Pre-paid Cards</i>	49
5.2.4. <i>Mobile Payments</i>	49
5.2.5. <i>Relevance to USAID and Implementing Partners</i>	51
5.3. LEGAL RISK	52
5.3.1. <i>Cash Payments</i>	52
5.3.2. <i>Electronic Funds Transfer</i>	53
5.3.3. <i>Pre-paid Cards</i>	54
5.3.4. <i>Mobile Payments</i>	54
5.3.5. <i>Relevance to USAID and Implementing Partners</i>	57

5.4.	OPERATIONAL RISK - GENERAL.....	57
5.4.1.	<i>Cash Payments</i> .....	57
5.4.2.	<i>Electronic Funds Transfer</i> .....	58
5.4.3.	<i>Relevance to USAID and Implementing Partners</i> .....	59
5.5.	OPERATIONAL RISK - INTEROPERABILITY .....	59
5.5.1.	<i>Electronic and Mobile Payments</i> .....	59
5.5.2.	<i>Relevance to USAID and Implementing Partners</i> .....	63
5.6.	OPERATIONAL RISK - CUSTOMER IDENTIFICATION AND AUTHENTICATION .....	63
5.6.1.	<i>Electronic and Mobile Payments</i> .....	64
5.6.2.	<i>Relevance to USAID and Implementing Partners</i> .....	68
5.7.	OPERATIONAL RISK – PROVIDER GOVERNANCE .....	68
5.7.1.	<i>Electronic and Mobile Payments</i> .....	69
5.7.2.	<i>Relevance to USAID and Implementing Partners</i> .....	71
5.8.	TECHNOLOGY RISK.....	71
5.8.1.	<i>Cash Payments</i> .....	72
5.8.2.	<i>Electronic Funds Transfer</i> .....	72
5.8.3.	<i>Pre-paid Cards</i> .....	73
5.8.4.	<i>Mobile Payments</i> .....	74
5.8.5.	<i>Relevance to USAID and Implementing Partners</i> .....	76
5.9.	REPUTATIONAL RISK.....	76
5.9.1.	<i>Cash Payments</i> .....	77
5.9.2.	<i>Electronic Funds Transfer</i> .....	78
5.9.3.	<i>Pre-paid Cards</i> .....	78
5.9.4.	<i>Mobile Payments</i> .....	80
5.9.5.	<i>Relevance to USAID and Implementing Partners</i> .....	81
<b>6.</b>	<b>EVALUATION OF PAYMENT ALTERNATIVES .....</b>	<b>82</b>
6.1.	EVALUATION PROCESS .....	82
6.2.	STEP 1 – IDENTIFY PAYMENT TYPE OPTIONS.....	82
6.3.	STEP 2 – DETERMINE RISK PROFILE FOR APPLICABLE PAYMENT TYPES .....	84
6.3.1.	<i>Risk Rating</i> .....	84
6.3.2.	<i>Risk Weighting</i> .....	84
6.3.3.	<i>Evaluating Risk for Cash</i> .....	85
6.3.4.	<i>Evaluating Risk for Electronic Funds Transfer</i> .....	86
6.3.5.	<i>Evaluating Risk for Pre-paid Cards</i> .....	89
6.3.6.	<i>Evaluating Risk for Mobile</i> .....	92
6.4.	STEP 3 – DECIDE ON SUITABLE LEVEL OF RISK .....	94
6.5.	STEP 4 – EVALUATE COST EFFICIENCY .....	95
6.6.	MOVING FORWARD .....	96
	<b>APPENDIX A: SUPPLEMENTAL INFORMATION.....</b>	<b>98</b>
A.1.	REGULATORY ENVIRONMENT .....	98
A.2.	MATURE PAYMENT METHODS.....	103
A.3.	ELECTRONIC AND MOBILE PAYMENTS.....	103
A.4.	RISK ANALYSIS AND MITIGATION .....	105
	<b>APPENDIX B: SOURCE LIST .....</b>	<b>107</b>
B.1.	OVERVIEW.....	107
B.2.	MATURE PAYMENT METHODS.....	108
B.3.	ELECTRONIC AND MOBILE PAYMENTS .....	108
B.4.	RISK ANALYSIS AND MITIGATION .....	111
B.5.	COUNTRY SPECIFIC .....	111
B.6.	OTHER.....	112

## ACRONYMS AND DEFINITIONS

ACH	Automated Clearing House
ADS	Automated Directives System
AML	Anti-Money Laundering
ATM	Automated Teller Machine
BCB	Banco Central do Brasil
BIC	Bank Identifier Code
BSP	Philippine Central Bank
CARD Act	Credit Card Accountability Responsibility and Disclosure Act
CBB	Central Bank of Brazil
CBK	Central Bank of Kenya
CCK	Communication Commission of Kenya
CDD	Customer Due Diligence
CFO	Chief Financial Officer
CFR	Code of Federal Regulations
CGAP	Consultative Group to Assist the Poor
CHIPS	Clearing House InterBank Payments System
CIP	Customer Identification Program
CMN	Convention for the Protection of National Minorities
CNP	Card Not Present
CPC	Consumer Protection Code
CTA	Cash Transfer Agency
CFT	Combating the Financing of Terrorism
CTIA	Cellular Telecommunications and Internet Association
DCHA	Democracy, Conflict and Humanitarian Assistance
DSS	Data Security Standard
e-CFR	Electronic Code of Federal Regulations
ECS	Electronic Certification System
EFT	Electronic Funds Transfer
EMV	EuroCard, MasterCard, and Visa
EPC	European Payments Council
EPP	Encrypting PIN Pad
FACTA	Fair and Accurate Credit Transactions Act
FATF	Financial Action Task Force
FCC	Federal Communication Commission
FDIC	Federal Deposit Insurance Corporation
FFP	Food For Peace
FIU	Financial Intelligence Unit
FMS	Financial Management Service
FPA	Federal Program Agency

FTC	Federal Trade Commission
GAO	Government Accountability Office
GDP	Gross Domestic Product
GSMA	GSM Association (association of mobile operators)
IBAN	International Bank Account Number
IC Card	Integrated Circuit Card
ID	Identification
IG	Office of Inspector General
IMF	International Monetary Fund
Imprest	A petty cash reserve account
IPAC	Intra-Governmental Payment and Collection
ISO	International Standards Organization
ITU	International Telecommunications Union
KEPSS	Kenya Electronic Payment and Settlement System
KSH	Kenyan Shilling
KYC	Know Your Customer
LOC	Letter of Credit
MDA	Brazilian Ministry of Agrarian Development
MDS	Brazilian Ministry of Social Development
MFI	Microfinance Institution
ML	Money Laundering
MMA	Brazilian Ministry of the Environment
MNO	Mobile Network Operator
MPFI	Mobile Payments Forum of India
MSME	Micro-, Small- and Medium- Scale Enterprise
MVNO	Mobile Virtual Network Operators
NACHA	National Automated Clearing House Association
NFC	Near Field Communication
NGO	Non-Governmental Organization
OAA	Office of Acquisition and Assistance
OCB	Brazilian Organization of Cooperatives
OCC	Office of the Comptroller of Currency
OFAC	Office of Foreign Assets Control
OFDA	Office of Foreign Disaster Assistance
OGC	Office of General Council
OMB	Office of Management and Budget
OTA	Over the Air
P2P	Person-to-Person
PA-DSS	Payment Application Data Security Standard
PCI	Payment Card Industry
PCK	Postal Corporation of Kenya
PED	PIN Entry Device

PIN	Personal Identification/Information Number
POI	Points of Interaction
POS	Point of Sale
RFP	Request for Proposal
SCMEPP	Society of Credit to Micro entrepreneurs and the Small Business Credit Company
SD	Secure Digital
SEBRAE	Brazilian Micro and Small Business Support Service
SEPA	Single Euro Payments Area
SIM	Subscriber Identity Module
SMS	Short Message Service
SPS	Secured Payment System
SWIFT	Society for Worldwide Interbank Financial Telecommunications
TSM	Trusted Service Manager
U.S.	United States of America
USAID	United States Agency for International Development
USDO	United States Disbursing Officer
USSD	Unstructured Supplementary Service Data
WBG	World Bank Group
WTO	World Trade Organization

## 1. OVERVIEW

The emergence of new electronic payment processing methods, including mobile phone banking and mobile payments, has created enormous potential for the global marketplace, offering convenience to consumers, new growth avenues to mobile carriers, differentiation to financial institutions, loyal customers to merchants, and a significant leapfrog opportunity for developing countries. Early successes in deploying such technology in a development context have demonstrated profound transformative potential in providing services to those Payment Beneficiaries who are traditionally difficult to reach in the provision of foreign assistance. In pilot programs in Africa, South America and Southeast Asia, for instance, development agencies and non-profit organizations have been able to more easily manage microfinance programs, distributing microloans directly to small entrepreneurs without the need to create a traditional bank account. It also helps such entities empower women in male-dominated cultures. Aid organizations are able to provide financial support directly to women through mobile devices or pre-paid cards, giving them direct control over their money and empowering them to positively impact the lives of their families. Electronic and mobile payments are also highly relevant to the delivery of government services. In Kabul, the Afghanistan national police have piloted a program to manage salaries through mobile banking services as a way to combat corruption and to reduce funds leakages by thirty percent.

Early successes in the application of electronic and mobile payments are encouraging and the potential benefits are well documented, both anecdotally and statistically.<sup>1</sup> In response, mobile network operators (MNOs) are beginning to provide mobile money payment systems in some developing nations, major payment networks are offering electronic payment options like pre-paid cards to specifically target the unbanked, and the enabling technology and regulatory frameworks are evolving to address the risks emerging out these new payments models. All of these trends converge to make the proliferation of emerging electronic and mobile payments ever more likely.

But developing a vibrant mobile payments ecosystem requires more than just technological progress. It is dependent on the concerted and collaborative efforts of aid organizations, government entities, MNOs, financial institutions, merchants and others to expand and standardize the use of such methods - in a manner that is mutually beneficial, sustainable and appropriately managed and regulated.

By establishing a set of common practices and precedents for the use of electronic and

---

<sup>1</sup> Sources for benefits of electronic and mobile payments:

- Dr. Ignacio Mas on Mobile Banking for the Poor. June 2010.
- It's Better Than Cash: Kenya Mobile Money Market Assessment, Loretta Michaels, USAID (2011)
- Bangladesh Electronic Funds Transfer Network (BEFTN) Operating Rules. Payment Systems Division - Department of Currency Management and Payment Systems. DCMPS Circular No. 09/2010 Bangladesh Bank.
- Update on Regulation of Branchless Banking in South Africa. Consultative Group to Assist the Poor (CGAP). January 2010.

## Overview: *Objective of this Report*

mobile payments for the disbursement of funding to Payment Beneficiaries in the developing world where doing so would further development objectives, the United States Agency for International Development (USAID) can help to accelerate trends in foreign assistance delivery that have the potential to address current challenges, including:

- The dangers and inefficiency that may be present in the use of cash- and paper voucher- based payments in some environments and in delivering financial assistance to Payment Beneficiary populations who may be vulnerable to violence while holding cash, such as women.
- Loss through illicit activities that is the result of an inability to effectively track the disbursement of cash payments.
- A lack of sustainable development solutions through fee-for-service models across agriculture, health and energy.
- Low financial services coverage amongst developing country populations, which limits economic development and growth.
- Limited transparency into and digital tracking of the final stage in the disbursement process (i.e., Payment Beneficiary's receipt and use of funds) which increases the risk of fund misuse (e.g., drug and human trafficking financing).

Electronic and mobile payments could be a powerful mechanism for supporting financial services expansion and increasing the reach of development support to the unbanked. However, cash payments may still be the most suitable and desirable option for some foreign assistance programs, and traditional bank and wire transfers are the safest methods for banked Payment Beneficiaries. Electronic and mobile payments have the potential to enhance the impact of a wide range of USAID programs, including microfinance, rural and agricultural finance, trade and competitiveness, social transfers and cash-for-work programs, and other economic growth programming. To date, however, a comprehensive strategy for assessing and evaluating payment alternatives in the developing world has not emerged. If USAID were to take the lead in developing such a strategy, it must be based on a thorough understanding of the existing regulatory landscape, best practices in the payments industry, and the contextual benefits and risks of each payment type in each specific program and country context.

### 1.1. Objective of this Report

The benefits of new electronic and mobile payment methods in support of USAID objectives to better serve the unbanked have been well-documented in other literature,<sup>2</sup> and that case will not be reiterated in this report. A practical strategy for evaluating an individual program or Mission environment for suitability of payment type, however, has not yet been proposed or considered in a structured manner. The purpose of this report is to set a baseline understanding of available payment alternatives and to establish a framework for evaluating those alternatives in consideration of the unique environment

---

<sup>2</sup> See footnote number 1.



## Overview: *Payment Types*

and risk profile of individual USAID programs or Missions.

USAID's policy-level support for the evaluation and adoption of electronic and mobile payments is somewhat fractured, with most adoption occurring at the Mission or program level. This is not surprising as the majority of electronic and mobile payment disbursements are being driven by USAID Implementing Partners, buoyed by the rapid development and proliferation of payment technology. USAID can play an active role in the evaluation of electronic and mobile payments for potential adoption as a facilitator and a broker between stakeholders at the Mission level, and as a supporter of standards and practices from headquarters.

The agency can also help Missions to determine if three important conditions exist when considering the adoption of electronic or mobile payments. First, at least one reliable payment provider must be operating in the local environment. Second, there must be an appropriate regulatory environment for payment transactions, at least the existence of a local government regulatory body that is able to support the creation of such an environment, or, in the absence of such a regulatory environment, sufficient internal controls on the part of the provider to compensate for the lack of government regulation or guidelines. Lastly, there must be sufficient reach among Payment Beneficiaries in the target market for alternatives to cash payments.<sup>3</sup>

Under these conditions, USAID is increasingly in a position to promote electronic and mobile payments expansion. The objective of this report is to provide a baseline understanding of:

- Existing and emerging payment types
- The regulatory environment and internal controls that govern payment transactions and payment providers
- The risk profiles of each payment type
- Strategies for risk mitigation related to each payment type

Using this analysis, the report provides an assessment framework that USAID can leverage to assist Missions and Implementing Partners when evaluating local environments with regard to the aforementioned conditions. This evaluation framework is a tool that will enable decision-makers to create a risk profile for available payment types as a means to select a proposed payment method. This analysis includes an assessment of project-level risk tolerance based on program objectives, and the balancing of program goals related to serving a Payment Beneficiary population against risks of payment failure.

### 1.2. *Payment Types*

The existing payment types evaluated in this report are cash and Electronic Funds Transfer (EFT). Cash payments include face to face payments in the form of physical currency or a

---

<sup>3</sup> Adapted from: USAID FS Series #9: Enabling Mobile Money Interventions, April 2010

## Overview: *Payment Types*

check, which make up a large portion of disbursements to end Payment Beneficiaries in the developing world. Cash is typically used if the Payment Beneficiary is unable to open a bank account, or if the banking system is undeveloped in the country.

EFT is the standard method for making Federal payments and the preferred method for disbursing funds to Payment Beneficiaries by USAID Missions and Implementing Partners, if Payment Beneficiaries have (or are able to obtain) a bank account. EFT describes any method used to transfer funds electronically. Most commonly this includes Automated Clearing House (ACH) interbank payments, wire transfers between entities (not necessarily limited to banks) and intra-bank transfers (movement of funds between accounts within a single bank).

Electronic and mobile payments are examined here as an alternative to the existing payment types; or at least an equally viable option for consideration by USAID Missions and Implementing Partners. The form of electronic payment method focused on in this report is pre-paid cards, which allow a Mission or Implementing Partner to disburse funds through the issuance of payment cards that are pre-loaded with a fixed amount of money. Electronic vouchers represent a restrictive type of pre-paid card where the Payment Beneficiary is provided with a set amount of funding to use for a particular purpose at participating merchants. The funding can be delivered through magnetic stripe or chip based plastic cards. Other forms of electronic payment, such as credit cards (that extend credit for purchases) or true debit cards tied to a current positive funds balance in a bank account are characteristic of developed countries and banked populations, and so are not evaluated here.

Mobile payments can include a number of technologies and methodologies. For the purposes of this analysis, the report focuses on remote payments and proximity payments. Remote payments provide flexibility in the kinds of transactions supported, allowing for person to person (P2P) payments and non-face to face payments. Proximity payments are used for point-of-sale transaction execution, typically between a business and an individual. They make use of Near Field Communication (NFC) technology and require physical proximity and Point of Sale (POS) infrastructure on the side of the business.

Figure 1 summarizes the benefits, limitations and suitability of each of these payment types. These will be discussed in further detail later in the analysis.

## Overview: Regulatory Environment

Figure 1: Payment Type Summary

Payment Type	Benefits	Limitations	Suitability
<b>Cash</b>	<ul style="list-style-type: none"> <li>• Flexible for Payment Beneficiary</li> <li>• Easy to use in countries with weak banking systems</li> <li>• Well established precedent for audit trail</li> </ul>	<ul style="list-style-type: none"> <li>• Susceptible to theft and fraud</li> <li>• Remote payments not possible</li> <li>• Weakest traceability to Payment Beneficiary</li> </ul>	<ul style="list-style-type: none"> <li>• Transactions where at least one party is unbanked</li> <li>• Face to face transactions</li> </ul>
<b>EFT</b>	<ul style="list-style-type: none"> <li>• Most comprehensively regulated payment type</li> <li>• Highly secure</li> <li>• Strongest traceability to Payment Beneficiary</li> </ul>	<ul style="list-style-type: none"> <li>• Not suitable for unbanked Payment Beneficiaries</li> <li>• Less reliable in countries with a weak banking system</li> </ul>	<ul style="list-style-type: none"> <li>• Transactions between two banked parties</li> </ul>
<b>Pre-paid Cards</b>	<ul style="list-style-type: none"> <li>• Supports financial access to under-banked population</li> <li>• Supports remote payments, such as internet payment</li> <li>• More secure than cash especially PIN enabled cards</li> <li>• Strong traceability to Payment Beneficiaries</li> <li>• Easy conversion to cash through ATMs</li> </ul>	<ul style="list-style-type: none"> <li>• Does not support P2P payments</li> <li>• Card payment infrastructure required</li> <li>• Signature based cards vulnerable to theft and fraud</li> </ul>	<ul style="list-style-type: none"> <li>• Commercial transactions where supporting POS infrastructure exists</li> <li>• Non face to face transactions (e.g., internet purchases)</li> </ul>
<b>Mobile: Remote</b>	<ul style="list-style-type: none"> <li>• Supports financial access to under-banked population</li> <li>• Device provides additional security features</li> <li>• Funds are more secure than in cash</li> <li>• Strong traceability to Payment Beneficiaries</li> </ul>	<ul style="list-style-type: none"> <li>• MNOs must be capable of providing some financial services</li> <li>• Payer and payee must both have mobile phones</li> <li>• Possible interoperability issues</li> <li>• May involve many players, introducing execution challenges</li> </ul>	<ul style="list-style-type: none"> <li>• Commercial POS transactions with no infrastructure requirement</li> <li>• P2P, P2G, G2P transactions</li> <li>• Non face to face transactions</li> </ul>
<b>Mobile: Proximity</b>	<ul style="list-style-type: none"> <li>• Leverages mature technology to create a relatively closed, secure system for transactions.</li> </ul>	<ul style="list-style-type: none"> <li>• Does not support non face to face transactions</li> <li>• NFC infrastructure required</li> <li>• Possible infrastructure compatibility issues</li> </ul>	<ul style="list-style-type: none"> <li>• POS transactions at business locations with supporting POS infrastructure</li> </ul>

### 1.3. Regulatory Environment

This report provides analysis of government regulation and guidelines, as well as industry standards that serve as a framework for payment transactions, as well as an evaluation of existing USAID guidelines as they pertain to transactions involved in the disbursement of foreign aid. The analysis of existing and emerging payment types in the following sections of this report includes an evaluation of international and national regulation, as well as the private and non-governmental standards and policies that are most relevant to the lawful and transparent transfer of development funds. Each of these is explored thoroughly later in the report. This section provides a summary of the regulatory bodies, regulations and

frameworks that informed this analysis.

### **1.3.1. Government Regulation Impacting Payment Systems**

Standards set by international bodies require implementation into local law by individual countries in order for the standards to be enforceable domestically. The principles and priorities established by such international standard-setting bodies create common expectations among public and private sector counterparts. This plays a very important role in the mitigation of risk associated with payment transactions, and as such, in the growth of private organizations that are able to provide electronic and mobile payment services.

When evaluating suitability of payment types for use at USAID Missions, it is important to understand the current regulatory regime with regard to financial transactions and payment entities. Throughout this report, local regulations and guidelines are reviewed where relevant in the context of relevant examples of payment system deployments. In addition, because they are important benchmarks for regulatory development in the developing world, and because they are highly relevant to USAID and Implementing Partners as the sender of funds, international and U.S. National Regulations have been reviewed. The following regulations and frameworks are examined in greater detail in this report:

- International / super national
  - Financial Action Task Force (FATF): Multinational body endorsed by the International Monetary Fund, World Bank, and United Nations, as the international standard-setting body for anti-money laundering (AML) and combating the financing of terrorism (CFT) safeguards. Specific FATF recommendations include preventative measures such as customer identification and transaction recordkeeping requirements.
- U.S. National Regulation
  - AML/CFT:
    - Banking Secrecy Act: Reviewed regulation pertaining to stored value cards.
    - U.S. Patriot Act: Reviewed U.S. Patriot Act and associated Customer Identification Program rule interpreting Section 326, to understand baseline U.S. standards for customer identification.
  - Consumer Protection:
    - Credit Card Accountability Responsibility and Disclosure Act (CARD) Act: Among other areas of regulation, the CARD Act provides guidelines around transparency of fees for pre-paid card holders.

## Overview: *Regulatory* Environment

- Electronic Funds Transfer Act<sup>4</sup> and “Reg. E”: Expands consumer protection from debit to pre-paid card to regulate statementing and receipt requirements for electronic funds transfer.
- Dodd-Frank Act: Includes provisions pertaining to fees on pre-paid cards.
- FDIC 12 CFR Part 205: Expands deposit insurance coverage to deposits held on pre-paid cards.

### **1.3.2. Private and Non-Governmental Sector Payments Standards and Policies**

Private sector entities and consortiums also play a significant role in encouraging the development of local regulation, guidelines and policy for the electronic and mobile payment industry. By aligning internal policy and industry best practices with international standards (i.e., personal information protection and fund tracking), significant progress has been made in mitigating real and perceived risks that exist today.

The following internal controls and guidelines are examined in greater detail later in this report:

- Network rules, e.g. VISA, MasterCard , American Express operating rules
- International standards bodies, e.g. EMV Co (EuroCard, MasterCard, and Visa) for chip cards, International Standards Organization (ISO) standards for commonly used payment protocols
- Bank and financial institution policies, controls, standards
- MNO policies, controls, standard (mobile phone payments)

### **1.3.3. USAID Funds Disbursement Guidelines**

In addition to external regulations, policies and guidelines, this report is intended to form part of the existing USAID operational framework. In this section the existing rules governing the disbursement of aid funding by USAID are summarized and analyzed in the context of payment type evaluation.

USAID funds disbursement and tracking guidelines establish circumstances for the transfer of funds to “recipients” through “awards,” and also from “recipients” to “sub-recipients” through “sub-awards.” The guidelines establish requirements for recipients and sub-recipients, who are treated as entities that have a contractual relationship with the U.S. government. The designations “recipient” and sub-recipient” represent specific terminology used in the funds disbursement guidelines. For the purpose of clarity in this report, recipients and sub-recipients (entities that have a contractual relationship with USAID and are disbursing funds) will be generally referred to as Implementing Partners.

---

<sup>4</sup> More detail on the Electronic Funds Transfer Act provided in Appendix A.2.

## Overview: *Regulatory Environment*

Internal USAID guidelines do not, however, articulate guidance with regard to Payment Beneficiaries of foreign assistance funds, or to the entities that support payment execution. This is highly relevant as it is the transfer of funds between recipients or sub-recipients to Payment Beneficiaries that commonly occurs in cash in development environments, and is the area in which electronic and mobile payments could potentially become more prevalent.

If USAID guidelines around awards and funds disbursement were used as a benchmark for evaluating the payment types, they could be said to represent guidelines for due diligence against electronic or mobile payment providers. It is not intended that payment providers necessarily meet each of these guidelines. For example, it is unrealistic to mandate that a mobile payments provider submit to an audit by USAID. However, it is realistic to expect that a mobile payments provider submit to an audit by a relevant local entity that could, in specific country contexts, include outside auditors or relevant regulatory agencies. As shown in this example, using the relevant ADS chapters as a baseline provides some common ground for the decision-maker, but should not necessarily be interpreted literally. Based on the ADS 630, Implementing Partners (direct recipients of USAID awards or funds) must be pre-screened to ensure that they have the following:

1. An internal financial management system that provides:
  - Records that identify adequately the source and application of funds.
  - Effective control over and accountability for all funds.
  - Comparison of outlays with budget amounts for each award.
  - Accounting records that are supported by source documentation.
2. Internal controls that comply with local laws and USAID contractual obligations.
3. Reporting and records maintenance practices that meet the following requirements:
  - Records are retained for at least three years.
  - Reporting on the disbursement of an award can be available within 90 days.
4. Are willing to submit to an annual audit.

Most Payment Beneficiaries of USAID development funds cannot meet the requirements listed above, nor are they uniformly required to do so, according to disbursement guidelines. For this reason, cash payments to Payment Beneficiaries are tracked with a much smaller transparency and audit requirement, typically backed with paper receipts authorized by the disbursing agent rather than an automated, digital accounting system entry. However, an electronic or mobile payment provider could help to mitigate the risk of disbursement of funds to Payment Beneficiaries by acting as a proxy to the Payment Beneficiary with regard to funds tracking. This concept will be revisited in later sections of this report.

The following USAID guidelines were reviewed and will be examined in detail throughout this report. They are also summarized in greater detail in Appendix A.1.:

## Overview: *Regulatory* Environment

- USAID ADS<sup>5</sup> Chapter 625 – Accounts Receivable and Debt Collection
- USAID ADS Chapter 630 - Payables Management
- USAID ADS Chapter 636 – Program Funded Advances
- 22 CFR<sup>6</sup> Part 226 – Administration Assistance Awards to Non-Governmental Organizations
- OMB<sup>7</sup> Circular A-133: Audits of States, Local Governments and Non-Profit Organizations
- Guidelines for Financial Audits Contracted by Foreign Recipients. Officer of the Inspector General.

---

<sup>5</sup> ADS stands for Automated Directives System

<sup>6</sup> CFR stands for Code of Federal Regulations

<sup>7</sup> OMB stands for Office of Management and Budget

## 2. STAKEHOLDERS

A stakeholder is defined as an actor, entity, or organization that is either directly impacted or maintains oversight with respect to the processing of USAID payments. The purpose of this section is to identify stakeholders, examine their interest and role, identify motivations, and the potential for future changes within the payments process. The complete process for programming, planning, obligating, and executing funds across the USAID ecosystem contains many actors, stakeholders, and organizations. However, for the purposes of this report, stakeholder relevance is bounded by the processing of USAID payments.

### 2.1. Direct Stakeholders

Direct stakeholders are defined as actors, entities, or organizations that are either creating, receiving, facilitating, transacting, or directly responsible for payments. These stakeholders are primary actors within the payment process and may be directly impacted by changes to payments processes or methods. Their motivations for change are varied and range from increasing transparency to increasing safety to decreasing cycle time. The bullets below provide specific descriptions for each of the direct stakeholder groups.

- **USAID Headquarters** – USAID Headquarters stakeholders include, but are not limited to the Office of the Chief Financial Officer (CFO), Office of General Counsel (OGC), Office of Acquisition and Assistance (OAA), and the Office of Inspector General (IG) Office. While individual interests, motivations, and responsibilities may differ, this stakeholder group is primarily responsible for planning, creating, overseeing and auditing payments within the USAID environment. Depending upon the type or destination of payment, this stakeholder group may create or enforce compliance language and encourage various methods for disbursement of funds to Payment Beneficiaries. In general, the majority of the relevant payments for this stakeholder group are currently electronic.
- **USAID Missions (or Bureaus)** – USAID Missions are the primary stakeholders in the execution of the program portfolio. They include program or technical offices, and may include representation from the aforementioned Headquarters stakeholder groups such as Contracts Officers or Controllers. USAID Mission stakeholders typically maintain the primary relationship with Implementing Partners and can also interact with Payment Beneficiaries such as local contractors or direct humanitarian assistance recipients. Their motivations include optimization of foreign assistance delivery, potential cost savings and ensuring the proper use of United States (U.S.) government funds. Also included in this category are USAID bureaus or offices that operate as part of USAID Headquarters, but also conduct foreign assistance programs in the field.<sup>8</sup>
- **USAID Implementing Partners** – This stakeholder group is defined as an actor,

---

<sup>8</sup> The full list of USAID Bureaus and offices can be found at <http://www.usaid.gov/who-we-are/organization/bureaus>.



## Stakeholders: *Indirect* Stakeholders

entity, or organization that possesses a business relationship with USAID as a part of program portfolio. This stakeholder group can include private companies, non-for-profit organizations, academic institutions, cooperatives, grantees, foreign governmental bodies, and other types of entities. More often than not, the Implementing Partners stakeholder group directly executes payments of USAID funds to Payment Beneficiaries across a range of activities. This includes the paying of local subcontractors, distribution of restricted stipends or vouchers, and the execution of program activities that require payments processing. Their motivations include efficient delivery of funds, safety of Payment Beneficiaries, completion of their stated program goals, and risk mitigation with respect to improper use of U.S. government funds.

- **Payment Service Providers** – This stakeholder group serves to facilitate or transact components of the payments process. Depending on the type of payment and methods used, this group is comprised of national and multinational banks, credit/debit card companies, MNOs, micro-finance institutions, or payment processors. They provide various methods or vehicles upon which the other stakeholder groups can participate in or execute the payment process. While they are direct stakeholders in the payments process, their motivation is often centered on the generation of revenue. This makes this group something of an interested party for the purposes of corporate gain, but not necessarily a stakeholder in the classic sense.
- **Payment Beneficiaries** – The Payment Beneficiaries stakeholder group is comprised of the actors or organizations at the final step in the payments process. In general, they are the beneficiaries of the payments and could be vendors, consumers, disaster-affected people, program beneficiaries or other end points on the payments process. It is reasonable to assume that this group is probably the most greatly impacted by a shift in payment processing methods or vehicles and is primarily motivated by the receipt and safety of funds.

### 2.2. Indirect Stakeholders

Indirect stakeholders are defined as actors, organizations, and entities that advocate, advise, develop standards, and conduct similar activities in relation to the payments process for international development. These stakeholder groups are not necessarily direct actors within the USAID payment process, but maintain interest and could potentially be impacted by changes to payment processes or methods. Their motivations for change vary from broad organizations goals such as financial inclusion to a mandate to provide generalized consumer protections. The bullets below provide specific descriptions for each of the stakeholder groups.

- **U.S. Department of the Treasury** – Among the Department of the Treasury's various roles relevant to USAID is the provisioning of U.S. government payment services through the Financial Management Service, implementing and enforcing domestic AML/CFT regulations and executive orders through the Financial Crimes

## Stakeholders: *Indirect* Stakeholders

Enforcement Network and the Office of Foreign Assets Control, supervising national banks through the Office of the Comptroller of the Currency, and leading U.S. participation in the work of the FATF OFAC administers and enforces economic and trade sanctions against countries, individuals, and organizations designated as a threat to the national security, foreign policy or economy of the U.S. All U.S. persons must comply with OFAC regulations, including all U.S. citizens and permanent resident aliens regardless of where they are located, all persons and entities within the U.S., all U.S. incorporated entities and their foreign branches. Certain programs also require foreign persons in possession of U.S. origin goods to comply.

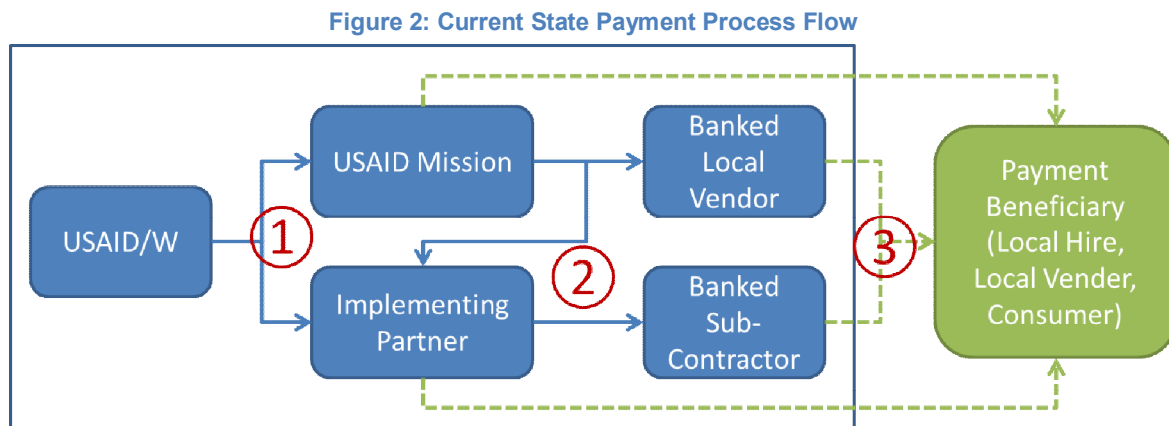
- **Other U.S. Government Compliance Organizations** – In addition to Treasury and the internal organizations of USAID, other bodies such as the Government Accountability Office (GAO), the Office of Management and Budget (OMB), and the Federal Trade Commission (FTC) have relevance to the USAID payment process. Tasked with oversight or standards development for the whole of government, they are not specifically focused on the USAID payment process, but either perform or provide analysis and guidelines on aspects of payment processing. As this document investigates the use of mobile payments, organizations such as the Federal Communication Commission (FCC) are also included within this group. Each of these compliance organizations provides binding regulations or general guidelines that must be considered when establishing policies or best practices for funds disbursements.
- **Global Standards or Regulatory Bodies** – This group includes the Basel Committee on Banking Supervision and Committee on Payment and Settlement Systems of the Bank for International Settlements, FATF, G-20, Organization for Economic Cooperation and Development, International Telecommunications Union (ITU), and the World Trade Organization. The organizations within this stakeholder group develop global standards and facilitate global coordination and cooperation among financial institutions with respect to payments processes. Their motivations include facilitating financial access and inclusion, international trade, sound banking practices, harmonized AML/CFT practices, and international cooperation among civil supervisory authorities and among criminal enforcement authorities. These organizations provide international best practices that can be used as a benchmark for institutional maturity and good governance when evaluating country-specific financial or payments practices.
- **Advocacy and Trade Organizations** – Comprised of organizations such as the GSM Association (GSMA) – an international association of MNOs – this stakeholder group is focused on advancing either specific initiatives or industries. Dependent on the payment method or vehicles employed, the population of this group may change. These organizations provide non-binding documentation on industry best practices and standardization guidelines. While global regulatory bodies focus on the aspects of country-specific maturity that can be directly influence by government, advocacy and trade organizations target the private sector as an actor for financial stability.

### 3. MATURE PAYMENT METHODS

As stated, the purpose of this report is to set a baseline understanding of available payment alternatives and to establish a framework for evaluating those alternatives in consideration of the unique environment and risk profile of individual USAID programs or Missions. In order to establish a baseline of accepted practices with regard to funds disbursement this section provides an analysis of payment methods that are mature and currently accepted by USAID through either compliance with disbursement guidelines or through established practice and precedent.

#### 3.1. Background and Governing Regulation

Figure 2 illustrates the typical payment process flow for USAID Mission support efforts. In this graphic, the solid blue lines represent payment processes that are governed by existing government guidelines and documented policy. The dotted green lines represent the flow of funds to Payment Beneficiaries of foreign assistance. This segment of the payment process is not governed by existing policy. However, for the payment types discussed in this section – EFT and cash payments – there is an established pattern or precedent through execution of successful audits or through extension of related guidelines, which establish alternatives to formalized rules and oversight.



#### 3.1.1. 1 – Flow of Funds from USAID Washington to Missions or Implementing Partners

Beginning at the left of this illustration, the first stage of funds disbursement (for the purposes of this analysis) is the award of funds between USAID headquarters and either a USAID Mission or an Implementing Partner that has a contract relationship or agreement with USAID for the provision of services. This part of the process is governed primarily by ADS Chapter 630.

ADS Chapter 630 on payables management sets forth the principles, requirements, and procedures that govern the examination, certification, and payment of basic vouchers, invoices, contract financing requests, claims, and other payment requests. This internal

## Mature Payment Methods: *Background* and Governing Regulation

policy establishes two primary methods for USAID to execute payments – direct payment and Intra-Governmental Payment and Collection (IPAC). EFT is the standard method for making Federal payments, and includes multiple methods for transferring funds electronically, including Fedwire, ACH transfers, IPAC and others.

### **3.1.2. 2 – Flow of Funds from Missions or Implementing Partners to Sub/Local Contractors**

The second stage of funds disbursement is between a USAID Mission or a USAID Implementing Partner and a local contractor or sub-contractor. (It may also include the disbursement of funds from a Mission to an Implementing Partner, depending on the origin of funds, however this distinction is not important for this analysis.) In most cases, this local contractor or subcontractor is banked. These secondary recipients are also covered by ADS Chapter 630 – specifically the guidelines with regard to sub-recipients and sub-awards of USAID funding. ADS Chapter 636 also covers this stage of the payment process.

ADS Chapter 636 on Program Funded Advances discusses payments made as advances such as a letter of credit, direct and special letter of commitment, and bank letter of commitment. The intent of this guideline is to prescribe policy on advances made to program-funded contracts and assistance awards and to ensure that organizations receiving USAID funds are provided appropriate financing for work carried out under agreements with USAID. Policy on program funded advance payments is dependent to some extent upon the type of obligation (or commitment) instrument under which the advance is made. ADS 636 guidelines apply to advances made against USAID-direct contracts, grants and cooperative agreements and host country direct aid contracts.

Approved methods for advancing funds are:

- Letter Of Credit (LOC)
- Periodic Treasury Check / ACH

The preferred method for financing contracts, grants or cooperative agreements for non-profit organizations is through Advance Payments (either LOC or Treasury check/ACH or wire transfer). The method of advance funding is specifically authorized in the contract, grant or cooperative agreement. For-profit organizations with a contract are expected to finance contract working capital requirements with their own resources, and to submit requests for reimbursement of applicable expenses with appropriate documentation to verify valid disbursement of funds.

### **3.1.3. 3 – Flow of Funds from Implementing Partners to Payment Beneficiaries**

The final stage of funds disbursement, as illustrated in Figure 3, is the payment of funds to a Payment Beneficiary. This may include local vendors, local individuals hired to support a project, individual service providers, consumers or other typically non-banked entities. As

## Mature Payment Methods: *Payment Methods*

indicated, the Payment Beneficiary may receive funds from the local contractor or sub-contractor, directly from the Implementing Partner or indirectly through a subcontractor of the local Implementing Partner.

The movement of funds to Payment Beneficiaries is not governed by existing USAID policy and there are no overarching guidelines for the tracking of such funds. However, Mission controllers, the USAID CFO's office and OAA procurement officers have established standard practices based on past audits of Implementing Partners and sub-contractors. There are two main scenarios:

1. Final Payment Beneficiary can accept EFT payment – In this scenario, funds are disbursed in accordance with established guidelines, treating the Payment Beneficiary as a sub-recipient of a sub-award.
2. Final Payment Beneficiary cannot accept EFT payments – In this scenario, cash payments are used and some form of paper receipt is provided to verify disbursement.

These two scenarios are the focus of the remainder of this section of the report.

### 3.2. Payment Methods

As established by existing guidelines, USAID uses several standard, EFT-based payment methods to disburse funds. These methods are most commonly used to execute intra government transfers or the transfers of substantial amounts to direct contractor and grantees. EFT is also leveraged, when possible, for disbursement of funds to Payment Beneficiaries in Mission countries, i.e. local organizations or companies who are direct service providers or grant recipients.

While it plays no role in intra government transfers, cash is currently a commonly leveraged payment method used to disburse funds to Payment Beneficiaries under the auspices of USAID programs and Missions.

In the following sections we will examine EFT and cash payments in greater detail, and the manner in which they are leveraged to disburse funds to Payment Beneficiaries.

#### 3.2.1. Electronic Funds Transfer / Wire Transfer

EFT is the standard method for making Federal payments. EFT includes any method used to transfer funds electronically, including Fedwire, ACH transfers, IPAC system, etc.

IPAC is used by Federal agencies to process transactions including transfers, collections and adjustments. The IPAC application's primary purpose is to provide a standardized inter-

## Mature Payment Methods: *Payment Methods*

agency fund transfer mechanism for Federal Program Agencies (FPAs).<sup>9</sup>

The U.S. Treasury has replaced the Electronic Certification System (ECS) with a Secured Payment System (SPS) for certifying and transmitting payment schedules for worldwide payments. Both systems are well-suited for making EFT payments to the U.S. bank accounts of vendors and employees without incurring any banking charges and posting cash collection transactions to the United States Disbursing Officer (USDO).<sup>10</sup>

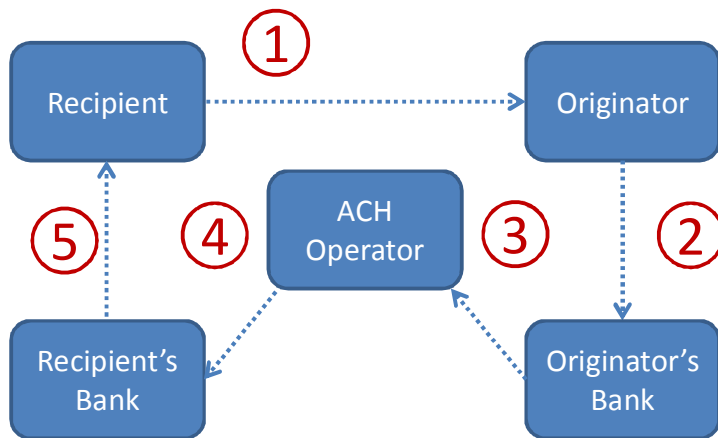
In assessing the suitability of different methods of EFT for disbursements to Payment Beneficiaries we will focus on wire transfers and EFT utilizing the ACH process as these represent open payment systems rather than those restricted to and secured by the government.

### Automated Clearing House (ACH)

The Automated Clearing House (ACH) is an EFT utility that provides for the interbank clearing of electronic payments and operates on a batch basis. Rules and regulations that govern the ACH network are established by NACHA (formerly the National Automated Clearing House Association) and the Federal Reserve. In the U.S. EFTs are regulated by the Electronic Funds Transfer Act.<sup>11</sup> This act defines the rights and responsibilities of EFT consumers and providers and limits consumers' liabilities arising from unauthorized transactions.

There is both a private electronic funds ACH operator, the Electronic Payments Network (EPN), which processes about 40% of transactions, as well as the Federal Reserve's centralized process, the Fed ACH. Similar mechanisms exist in all developed payment markets. Figure 3 illustrates a typical process for an ACH push transaction.

Figure 3: Automated Clearing House Payment Process Flow



<sup>9</sup> USAID. ADS Chapter 630. Payables Management. November 30, 2011. Page 19.

<sup>10</sup> Ibid, page 15

<sup>11</sup> More detail on the Electronic Funds Transfer Act provided in Appendix A.2.

## Mature Payment Methods: *Payment Methods*

1. The Recipient of the ACH credit/debit entry authorizes the Originator to initiate a credit/debit entry (note: the recipient can both receive and make a payment in this process). Authorization from a recipient of an ACH transaction is required before a transaction can be initiated.
2. The Originator then initiates an ACH debit/credit entry.
3. The Originator's Bank forwards the debit/credit entry to the ACH operator.
4. The ACH operator submits the file to the Recipient's Bank
5. The Recipient's Bank receives the debit/credit entry from the ACH system and credits or debits the Recipient's account.

On the consumer side, the ACH process is typically used in the U.S. for payments from the government to an individual, e.g. social security payments, or for payments by consumers of monthly obligations such as mortgage payments. ETF payments conducted using the ACH process require that the originator and recipient have a bank account and that an established functioning clearing house exists. In the case of payments to Payment Beneficiaries of aid in the developing world, the appropriate infrastructure in terms of bank systems and Payment Beneficiary accounts regularly does not exist. As such, this is not a viable option for the disbursement of funds to Payment Beneficiaries.

### Wire transfer

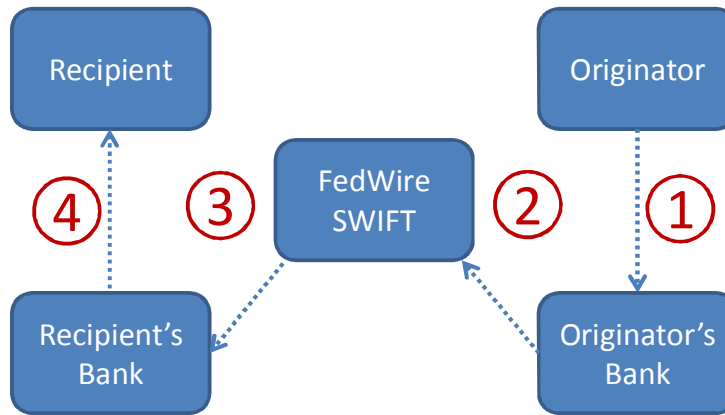
Wire transfer is a method of EFT that facilitates the transfer of funds from one bank account to another. It is a secure and compliant payment mechanism with both sender and recipient identified as bank account holders.

In the U.S. wire transfer payments are executed through Fedwire or through the Clearing House InterBank Payments System (CHIPS). Most international transfers are executed through the Society for Worldwide Interbank Financial Telecommunications (SWIFT), a nonprofit cooperative of member banks serving as a worldwide interbank payments network. It is the primary message system employed by financial institutions worldwide to transmit either domestic or international payment instructions.

International transfers involving the U.S. are subject to monitoring by the OFAC, which monitors information provided in the text of the wire to ascertain whether money is being transferred to terrorist organizations or countries or entities under sanction by the U.S. government. If a financial institution suspects that funds are being sent from or to one of these entities, it must block the transfer and freeze the funds, making this a relatively secure payment method. Figure 4 illustrates the typical process for a wire transfer transaction.

## Mature Payment Methods: *Payment Methods*

Figure 4: Wire Transfer Payment Process Flow



1. The Originator issues a payment instruction to its bank providing the recipient's information including International Bank Account Numbers (IBAN) and Bank Identifier Codes (BIC) as well as the amount.
2. The Originator's bank transmits a message, to a secure system (such as SWIFT or Fedwire).
3. The Fedwire or SWIFT system transmits the message to the recipient's bank, requesting that it execute payment according to the instructions given. (If no direct relationship exists between the banks, intermediary banks, also known as correspondent banks, may be used).
4. The recipient's bank credits the recipient's account and the payment transaction is complete.

Wire transfers are habitually used for business-to-business transactions and, in the field, this is the most well-established method of distributing funds to Payment Beneficiaries by USAID Missions and Implementing Partners – and the method around which USAID has the most comprehensive guidelines. However, this form of EFT can only be used to disburse funds to Payment Beneficiaries in a country with a relatively mature banking system. In addition, it is only feasible for the execution of transactions between two entities that have bank accounts. Any Payment Beneficiaries who are unable to obtain a bank account would not be able to receive payments via wire transfer.

### Intra-Bank Transfer

In many USAID Mission environments, where the banking system is not mature enough to support bank-to-bank ACH or wire transfers, USAID Missions and Implementing Partners will sometimes use intra-bank funds transfer. This process is, essentially, a bank-assisted cash transaction but it does support more robust funds tracking than cash-only payments.

In an intra-bank transfer, the Mission or Implementing Partner will require that Payment Beneficiaries open a bank account at the same bank that is holding the payer's capital funds. Payments will be executed (typically in person with representatives for both parties



## Mature Payment Methods: *Payment Methods*

present) by signing a funds transfer between accounts equal in value to a given invoice or procurement document.

For this form of EFT, the traceability of payments to Payment Beneficiaries is as reliable as other intra-bank payments. However, intra-bank transfers (those that are not also ACH transfers) are typically leveraged when the banking sector is less developed. In addition, intra-bank payments are vulnerable to fraud or corruption internally – particularly in instances where bank transaction processes are manual and/or paper based. This is regularly the case in post-conflict areas (e.g., Afghanistan and Iraq).

In short, while intra-bank transfers provide better payment traceability than cash, and significantly more security from the perspective of the payee, there are still notable weaknesses related to process execution and the reliability of documentation.

### **3.2.2. Cash Payments**

Cash continues to be the preferred payment tool for consumer-level transactions. Even in highly developed payments markets such as the U.S., cash remains among the most popular payment methods; in fact 28% of consumer payment transactions in 2009 were conducted using cash.<sup>12</sup> The popularity of cash extends to its wide use in developing countries where the majority of the population is not banked or under-banked, and a large percentage of disbursements to Payment Beneficiaries of USAID development dollars are executed in cash. This category of payments, for the purposes of this report, also includes any kind of check that can be cashed by a Beneficiary, even if he or she does not have a bank account, as this payment method has a risk profile very similar to that of cash.

The use of cash to disburse funds has clear benefits for Payment Beneficiaries. Cash allows for a great deal of flexibility in how funds are used (as long as transactions can be executed face to face), and there are no limitations on access to funds once they are transferred to the Payment Beneficiary. However, there are clear risks for the Beneficiary and the Implementing Partner (the stakeholder disbursing funds on behalf of USAID) including: the security of funds, misallocation of monies, theft, and traceability of payments to Payment Beneficiaries.

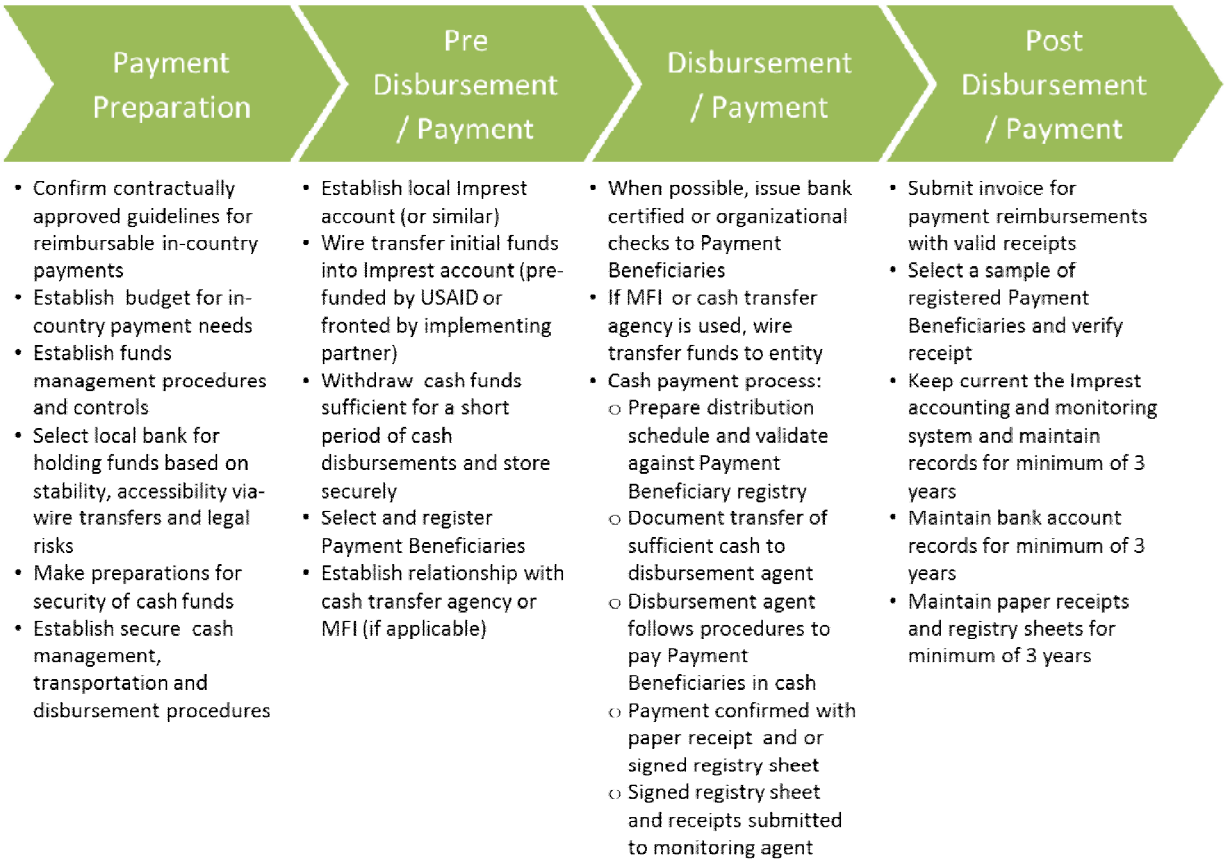
As a result of the risks and limitations, a robust, and commonly accepted, set of standard cash payment practices has been established through precedent of acceptance in USAID audits, and through interpretation of USAID funds management guidelines. In practice, implementation procedures vary, tailored to the unique local country environment. However, cash payment disbursement activities can be categorized into four stages. These are depicted in Figure 5 below.

---

<sup>12</sup>Survey of Consumer Payment Choice 2009, published by Federal Reserve Bank of Boston

## Mature Payment Methods: *Payment Methods*

Figure 5: Cash Payment Process Flow



**1. Payment Preparation** – This first stage includes all of the activities that occur before funds are made available in-country.

- The Implementing Partner or other disbursing entity will, if possible, select a local bank to hold funds sufficient for a designated period of program activity.
- Bank selection will be based on an assessment of institutional stability, ability to receive wire transfers for funds replenishment and a number of other tax and legal issues.
- The partner will establish documented guidelines for the kinds of payments that are reimbursable by USAID as well as procedures and preparations for the secure storage and transportation of cash.

**2. Pre-Disbursement/Payment** – This stage involves bringing funds into the country in preparation of disbursements to Payment Beneficiaries and preparing to execute cash payments.

- The Implementing Partner will wire transfer funds into the local Imprest account (petty cash reserve account). If the partner is operating under a grant vehicle, funds will typically be advanced by U.S. Treasury (who holds USAID funds) under a letter of credit. Private sector Implementing Partners operating under a services contract are typically expected to fund Imprest from their

## Mature Payment Methods: *Payment Methods*

own cash reserves and they invoice for approved expense types.

- Payment Beneficiaries will be pre-selected, registered and verified for eligibility under the program. This supports later monitoring and evaluation of effective disbursement.
- If applicable, the Implementing Partner may use a microfinance institution (MFI) or other cash transfer agency (CTA) to ultimately distribute funds to Payment Beneficiaries. If so, a contract would be established with this entity, and a certain amount of funds will be wire transferred to them from the Imprest account.
- If direct cash payments are to be made, the partner will withdraw cash sufficient for an individual disbursement period and store it in a secure environment, likely in a safe of some kind.

### **3. Disbursement/Payment** – This stage includes all activities around the physical disbursement of funds to Payment Beneficiaries.

- When possible, many Implementing Partners try to avoid personally transporting and disbursing physical currency. They will, if Payment Beneficiaries are capable of proving their identity, issue a check that can be cashed at a bank, or work with a cash transfer agent that will serve as a quasi-bank from which Beneficiaries can withdraw funds.
- For physical cash payments, the Implementing Partner will prepare and validate the disbursement schedule against the Payment Beneficiary registry and follow documented processes and security procedures for cash transfer, verifying chain of ownership throughout.
- At disbursement, a registry sheet will be signed by the Payment Beneficiary when they receive funds, and countersigned by the Implementing Partner's monitoring agent. If applicable (depending on the type of payment) a paper receipt for goods or services will be collected.

### **4. Post-Disbursement/Payment** – This stage includes activities related to verification of successful receipt of payment by Payment Beneficiaries, and preparation and maintenance of audit trail documentation.

- The Implementing Partner maintains an accounting of the Imprest account and updates it following payment execution. A budget is also maintained with projected disbursements, and the accounting process should include reconciliation against budget.
- Implementing Partners will invoice for reimbursable expenses using receipts and signed registry sheets, or will use this same evidence to validate disbursements against a letter of credit advance.
- Partners will have a monitoring and evaluation methodology to verify that payments were received by Payment Beneficiaries and used as expected, if applicable. This may include selecting a sample of registered Payment Beneficiaries and following up to ensure funds were received.
- All applicable audit trail records are maintained for a minimum of 3 years,

## Mature Payment Methods: *Payment Methods*

including Imprest accounting records, registry sheets, bank records and paper receipts.

While there is no formally documented process for the approval of payment to Payment Beneficiaries by USAID, existing guidelines related to the responsibilities of award recipients (Implementing Partners, most commonly) is generally applied. More specifically, the responsibility and liability for proper disbursement of funds – and for verification that payments were received by intended Payment Beneficiaries – lies with the Implementing Partner. USAID ADS guidelines and the Electronic Code of Federal Regulations (e-CFR) related to administration of non-governmental organization (NGO) operated USAID programs provide instruction to Implementing Partners on their responsibility with regard to funds management. It is commonly accepted interpretation of these regulations, policies and guidelines that serves as the basis for the practices described above.

It is very likely that, despite the growth of cash alternatives, many Implementing Partners will continue to employ cash payments for the disbursement of foreign assistance monies. In some circumstances, those where the majority of Payment Beneficiaries are unbanked and non-cash payment alternatives are unavailable, cash may still be the most viable or reasonable payment type.

The ideal scenario would be one where Implementing Partners and USAID Missions could determine if cash payments are the best option for that program, on a case-by-case basis after a thorough evaluation of all possible options, consideration of Payment Beneficiary needs, assessment of development program objectives and an evaluation of environmental readiness, . In the following section, electronic and mobile payment methods are examined in the context of USAID's unique needs and circumstances to facilitate such an evaluation.

## 4. ELECTRONIC AND MOBILE PAYMENTS

As stated, the purpose of this report is to set a baseline understanding of available payment alternatives and to establish a framework for evaluating those alternatives in consideration of the unique environment and risk profile of individual USAID programs or Missions. The previous section of this report established a baseline of accepted practices with regard to funds disbursement and an analysis of mature payment methods. This section provides an introduction to electronic and mobile payment methods and addresses the following questions:

- How do mobile and other electronic transactions work?
- What are the various forms of mobile and other electronic payment types?
- Who uses these payment types?
- What is the amount of money transferred annually using these payment types?
- What is the difference between “cashless” and “electronic payments?”
- What is the current state of regulation, standards, and governing bodies for these payment types?

The objective of USAID is to introduce additional payment type options to programs to increase the effectiveness and security of payment transactions while maintaining the existing funding processes from USAID Washington to the USAID Mission and Implementing Partner or local contractor. Each of the examined payment types in this section is grounded in the context of the USAID operating environment as well as the assumption that existing funding processes will be unchanged. Essentially, this document assumes that additional payment transaction methods will be made available to Payment Beneficiaries and that additional guidelines will be provided to leverage these new payment methods.

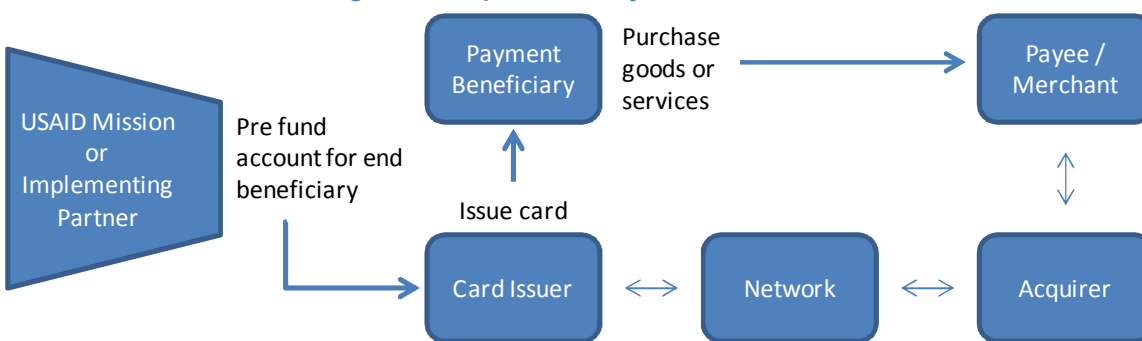
Within this context, we examine two additional payment types available for disbursement to Payment Beneficiaries who may or may not maintain a banking relationship. Those payment types are pre-paid cards and mobile.

### 4.1. Electronic Payments: Pre-paid Cards

Pre-paid cards have gained in popularity in developed and developing markets alike as they allow un-banked customers to participate in electronic payments. Pre-paid cards are mostly magnetic strip based. Additionally they may feature an embedded chip or microprocessor that allows the card to store information. Both magnetic strip and chip cards (also commonly referred to as “smart cards”) can be secured with a Personal Identification/Information Number (PIN). Pre-paid cards typically operate in the so-called “four party model” of consumer, issuer, merchant, and acquirer, with a network providing the connection between participants. Figure 6 describes how each of these actors contributes to the execution of a transaction.

## Electronic and Mobile Payments: *Electronic* Payments: Pre-paid Cards

Figure 6: Pre-paid Card Payment Process Flow



### Description of Actors:

- **Payment Beneficiary (Cardholder)** – Generally, the end beneficiary of a payment or benefit from USAID. The entity intended to spend the disbursed funds.
- **Card Issuer** – A bank or other pre-paid provider that physically issues the card as well as maintains an account of available funds.
- **Network** – The provider of payment processing infrastructure, connecting all other actors in the process.
- **Acquirer** – A bank or other institution that provides POS devices to payee (merchant) and connects the payee to network. Underwrites merchant risk.
- **Payee** – The merchant or destination of funds spent by a Payment Beneficiary.

Pre-paid cards can be used for the purposes of disbursing funds beyond a USAID Mission or Implementing Partner. A list and description of pre-paid card uses is presented below. This list is not intended to be exhaustive, but does provide relevant examples that demonstrate the applicability of the payment type to USAID activities.

- **Example 1: Local Procurements in Post-Conflict** – When operating in post-conflict environments, procuring locally available goods (such as office supplies or perishables) can be a challenge. From a security as well as fraud reduction perspective it may be beneficial to use pre-paid cards instead of cash. The safety of either local employees or advisors is moderately increased by holding the funds on a card rather than cash. In addition, there is an electronic record of the transaction and the possibility to cancel a card if in fact theft does occur. However, potential challenges include the reliance on local vendors to have functional POS devices that support pre-paid cards.
- **Example 2: Stipends or Vouchers** – Instead of providing cash stipends to Payment Beneficiaries, an Implementing Partner provides pre-paid cards. Vouchers and stipends also can be used to pay stipends or *per diems* for travel or participation in workshops or trainings. Advantages include controls for pre-paid card spending at the merchant category level to limit transactions to appropriate merchants. These controls allow pre-paid cards to replace vouchers and act as “Electronic Vouchers”.
- **Example 3: Local Employees Salaries** – Local employees of Implementing Partners could be paid using pre-paid cards. The ability of pre-paid cards to be reloaded or

## Electronic and Mobile Payments: *Electronic* Payments: Pre-paid Cards

funded remotely provide for potential advantages. In addition, governments and government agencies can realize significant cost savings by moving to pre-paid card from a check based system (e.g., U.S. Federal Government pays Social Security, SSI, Veterans, and Indian Trust Fund using pre-paid cards).<sup>13</sup>

### **4.1.1. Description: Pre-paid Cards**

This section describes the process by which a pre-paid card is both established and utilized. For the purposes of disbursing funds to Payment Beneficiaries, the term “customer” conceptually includes two actors. The first actor is the USAID Mission or Implementing Partner who is funding the Payment Beneficiary. These actors are responsible for paying the Issuer to establish an account. The second actors in the role of “customer” are the end Payment Beneficiaries themselves, who would be able to spend the funds allocated to the card.

#### *Distribution channels*

While pre-paid cards operate on global branded payment card networks, there are additional stakeholders in the pre-paid value chain, mainly in the distribution and program management functions. In both developed and developing markets the distribution channels regularly involve retailers and kiosks. This allows for unbanked Payment Beneficiaries to execute transactions that would have otherwise required access to credit or a bank account. For example, Payment Beneficiaries who formerly received cash can use pre-paid cards to access Internet or telephone-based merchants without having to qualify for credit or maintain a bank account.

#### *Account set-up*

USAID Missions or Implementing Partners provide Payment Beneficiary information to the Issuer, a bank or a pre-paid provider, and make a deposit to open a pre-paid account. This deposit can be made through a bank transfer or a local agent or merchant. There are several approaches to handling the deposit the customer makes: the bank may maintain pooled reserve accounts with sub-accounts or may set up individual accounts.

Payment Beneficiaries are then issued a card which may be a closed loop card, for example a retailer gift card, or an open loop card, also known as General Purpose Reloadable card, bearing the network logo (e.g., VISA, MasterCard, China Unionpay etc.). The card may then be used to make purchases or withdraw funds similar to other payment card types (e.g., debit, credit etc.).

### **4.1.2. Uses, Limitations, Risks, and Mitigants: Pre-paid Cards**

---

<sup>13</sup> Public Benefits and Wages on Pre-paid Cards: Protecting Against Hidden Fees and Identity Theft, NCLC Consumer Rights and Litigation Conference, November 2010

## Electronic and Mobile Payments: *Electronic* Payments: Pre-paid Cards

The pre-paid card payment type offers USAID Missions or Implementing Partners an alternative to cash disbursements to Payment Beneficiaries. However, as with any technological or process advancement there are use cases, limitations, risks, and potential mitigants to risks that must be considered prior to making a decision. Risks and mitigation strategies will be introduced here, and discussed in more detail in the Risk Assessment and Mitigation section of this report.

### Uses for Pre-paid Cards

- **Point of Sale Transactions** – Pre -paid cards are well suited for POS transactions. While there is a notable limitation in that a vendor or merchant must have POS infrastructure in place, the pre-paid card allows for convenient as well as electronically traceable transactions.
- **Non Face to Face Transactions** – In comparison to cash, pre-paid cards can more effectively support transactions where parties are not physically co-located. These types of transactions typically occur over the Internet or telephone and allow for access to goods and services that would be unavailable for purchase with cash.
- **Cash Withdrawals** – Depending on the makeup of actors in the transaction model, pre-paid cards can provide relatively easy access to cash through ATMs.

### Limitations of Pre-paid Cards

- **Network** – Pre-paid cards generally function within an open loop network (e.g., VISA, MasterCard, China Unionpay etc.). In order to take part in a transaction all actors need to be participants in the network. It may be the case that in some developing countries, the types of actors required to execute a transaction may not be present.
- **Person to Person Payments** – P2P payments are not part of core functionality.
- **Infrastructure** – Pre-paid cards rely on a physical network infrastructure that might not exist on a nationwide basis in developing markets. As authorization is performed in real time, they also require a stable and secure electricity supply – the exception being smart cards or stored value cards that do not need real-time bank authorization to complete a transaction.
- **Point of Sale Devices** – In order for Payment Beneficiaries to spend the funds allocated to the pre-paid card, merchants and/or vendors must have matching POS devices. Alternatively, the card could be configured for cash out via an ATM, but this would instead require a viable electronic banking infrastructure to be in place.

### Risks for Pre-paid Cards

- **Theft and Loss** – Pre-paid cards can be issued as PIN or signature enabled cards. If issued as magnetic stripe signature enabled cards, as is common today, they are exposed to the same theft risk as other magnetic stripe signature cards (e.g., fraud



through falsified signature).

- **Money Laundering** – Without adequate regulation, supervision, and transaction monitoring pre-paid cards, like many payment instruments, can be used as an effective vehicle for money laundering. The combination of ATM functionality, portability, and potential for anonymity and high load limits may create an opportunity for criminals to convert illicit cash into laundered funds. This is exacerbated by the international functionality of pre-paid cards. This risk was reaffirmed in a recent report by FATF that describes how pre-paid card functionality could be used for illicit activities. “Pre-paid cards can be designed to afford the customer absolute anonymity while maintaining a high degree of functionality. For example, some pre-paid card issuers attract customers with anonymous pre-paid cards with no or high loading and transaction limits.”<sup>14</sup>

#### Mitigation Strategies for Pre-paid Cards

- **Multi Factor Authentication** – Adding a PIN that is only known to and safeguarded by the cardholder limits the value of the card to unauthorized third parties. Another layer of security can be added by delivering pre-paid accounts via a mobile device: the phone’s SIM card can act as another authentication factor.
- **Fraud Monitoring** – Fraud monitoring systems will flag suspicious activities and allow banks to suspend usage of the card until a cardholder has been able to demonstrate that he is the authorized user. Location based intelligence from GPS enabled phones can be also be used to monitor transactions for evidence of fraud.
- **Know Your Customer (KYC) Policies** – Performing some level of customer due diligence and registering users of pre-paid cards will mitigate the risk that pre-paid cards are used for money laundering.
- **Network Regulations** – All card networks provide a comprehensive transaction dispute management system. The dispute management system is an arbitration system based on network rules. All network participants must adhere to network rules, and network arbitration decisions are final. Dispute management procedures allow cardholders to object to transactions that they believe have been incorrectly or fraudulently applied to their accounts.
- **Closed Loop Networks** – Closed loop networks can be set up that carry less of a cost burden than open loop networks and can be customized to the conditions in the target country. As an example, USAID Missions or Implementing Partners could establish the equivalent of a vendor or good-specific gift pre-paid card that could only be used for a defined set of transactions.

#### **4.1.3. Regulation: Pre-paid Cards**

As the pre-paid card payment type sits on top of relatively mature infrastructure, the regulatory environment for has two major goals:

---

<sup>14</sup> FATF Money Laundering and New Payment Methods, October 2011, page 24)

## Electronic and Mobile Payments: *Electronic* Payments: Pre-paid Cards

1. Consumer protection
2. Prevention of money laundering and terrorist financing

It is important to note that these goals are not specific to pre-paid cards and thus the applicable regulatory bodies may address additional payment types. Additionally, these issues are globally relevant and not specifically germane to emerging markets.

Within the U.S., regulation currently happens at the Federal and State level. We will be reviewing those briefly below as they draw attention to features of the pre-paid product that should be considered by Implementing Partners in other markets as well. At the same time, there are relevant international bodies that issue recommendations to various national regulators to incorporate in their rulemaking; these can be leveraged for the purposes of using pre-paid cards within the context of Payment Beneficiaries. As pre-paid cards have existed in the U.S. for some time, the intent of their inclusion in this document is to serve as a frame of reference for developing countries who may be investigating national regulation.

### *International / super-national bodies*

An international or super-national body is defined as an organization that provides guidelines, standards, or policy applicable to more than one country. USAID operates in many countries around the world and as such, the local regulatory environments can not necessarily be generalized. However, for the purposes of understanding the applicability of the pre-paid card payment type in a specific country, the international/super-national bodies remain relevant.

### *Financial Action Task Force*

The FATF is an inter-governmental body that sets standards and develops policies to combat money laundering and terrorist financing. The FATF includes 36 members representing global financial centers, 9 FATF-style regional bodies that include almost all of the rest of the world, and a large group of observers including the International Monetary Fund, United Nations, World Bank and many regional development banks. The FATF recently updated and revised its standards, which are titled: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation - the FATF Recommendations. There are 40 Recommendations, which address preventative measures (e.g. customer identification, transaction recordkeeping, and suspicious transaction reporting requirements), supervisory and enforcement practices, and international cooperation obligations. These recommendations are intended to provide a complete set of countermeasures against money-laundering and terrorist financing. Many of the Recommendations allow a risk-based approach to implementation, which requires an objective assessment of the relevant money laundering and terrorist financing threats in the country and the potential threats associated with specific products, services, and customers. The FATF conducts peer assessments to monitor compliance with the

## Electronic and Mobile Payments: *Electronic* Payments: Pre-paid Cards

Recommendations and helps to coordinate multilateral political and economic pressure to support strengthening jurisdictional AML/CFT regimes.

As USAID examines the applicability of the pre-paid card payment type through the lens of AML/CFT it can be difficult to determine in which countries national regulators adhere to the guidelines provided by FATF. To aid in this task, the FATF provides a routinely updated list of high-risk and non-cooperative jurisdictions via their website.<sup>15</sup> The current list is provided in Appendix A.3.

In late 2010, the FATF updated a report entitled “Money Laundering Using New Payment Methods”<sup>16</sup> that among other payment types, examines the use of pre-paid cards for the purposes of money laundering and terrorist financing. Based on a review of case studies, existing literature, and interview responses from 37 global jurisdictions, the report identified areas where their existing standards did not adequately address the pre-paid card payment type.<sup>17</sup> Specifically, the report proposes additional guidelines concerning the use of third parties such as agents or program managers in the distribution of pre-paid cards as they currently fall out of scope of existing guidelines.

### U.S. Federal and State Regulations

The pre-paid card market within the U.S. is significant at \$333 Billion in value loaded in 2009<sup>18</sup> and continues to grow at double digit rates.<sup>19</sup> As such, multiple Federal and State regulations exist. As this document is intended to support decision-making for Payment Beneficiaries in foreign countries, these regulations have been provided in an abbreviated form, but can be used as a reference point as developing countries create their own national regulations. Additional detail can be found in Appendix A.3.

- In August 2006, the Federal Reserve Board issued amendments to Regulation E, clarifying that the regulation covers payroll cards.<sup>20</sup>
- In a ruling published in November 2008, the Federal Deposit Insurance Corporation (FDIC) extended insurance coverage to deposits on pre-paid cards.<sup>21</sup>
- The Credit Accountability, Responsibility and Disclosure Act of 2009 (CARD Act), contains provisions specifically applying to pre-paid cards in three categories, general-use pre-paid cards, gift certificates, and store gift cards.<sup>22</sup>
- The Dodd-Frank Act established rulemaking authority for the Federal Reserve over

---

<sup>15</sup> The full list can be found at the following address: [http://www.fatf-gafi.org/pages/0,3417,en\\_32250379\\_32236992\\_1\\_1\\_1\\_1,00.html](http://www.fatf-gafi.org/pages/0,3417,en_32250379_32236992_1_1_1_1,00.html)

<sup>16</sup> <http://www.fatf-gafi.org/dataoecd/4/56/46705859.pdf>

<sup>17</sup> Ibid, Page 8.

<sup>18</sup> Mercator Advisory Group,

[http://www.mercatoradvisorygroup.com/index.php?doc=Prepaid&action=view\\_item&id=519&catid=16](http://www.mercatoradvisorygroup.com/index.php?doc=Prepaid&action=view_item&id=519&catid=16)

<sup>19</sup> The 2010 Federal Reserve Payments Study, Noncash Payment Trends in the United States: 2006 – 2009, page 4

<sup>20</sup> FEDERAL RESERVE SYSTEM 12 CFR Part 205 [Regulation E; Docket No. R-1377] Electronic Fund Transfers)

<sup>21</sup> *FDIC Deposit Insurance*: The Federal Deposit Insurance Act

<sup>22</sup> *Card Act*: The Credit Accountability, Responsibility and Disclosure Act of 2009 (CARD Act)

## Electronic and Mobile Payments: *Mobile Payments*

debit card interchange. Certain pre-paid cards are included in the provision.<sup>23</sup>

- The Office of the Comptroller of Currency (OCC) has addressed store value cards in OCC Bulletin 2006-34, asking issuers to ensure they adequately inform consumers and disclose certain information.<sup>24</sup> See Appendix A.3. for a list of disclosure requirements supported by OCC.

### 4.2. Mobile Payments

In the last decade, mobile payments have emerged as a new method of transaction and have led to new payment systems, leveraging the explosive growth of mobile phones. A driving factors behind the emergence of mobile payments in developing markets has been increased consumer convenience, the ability to deliver more integrated and seamless merchant solutions, and improved general flexibility and security in the transport and ownership of funds. As mobile payments are examined for use within the USAID program portfolio, the advantages over cash may include Payment Beneficiary safety, increased traceability and accountability in transaction processing and more efficient delivery of foreign assistance.

Developing a vibrant mobile payments ecosystem that brings together MNOs, financial institutions, merchants, and a host of others to let Payment Beneficiaries use their mobile devices to receive disbursements and in turn, pay for goods and services is no easy task. Industry players are optimistic, but the challenges are daunting. Mobile payments have not yet reached the state of maturity of credit card or pre-paid card payments common in developed economies. In fact, there is not a standard definition of what constitutes a mobile payment.

The term mobile payments means different things to different people. There are remote payments and proximity payments. There are carrier-based billing and downloadable wallets that enable existing credit cards. There are cloud based payments and many more permutations. For the purposes of this report, the content is focused narrowly on mobile payment methods – remote and proximity – currently in use or under consideration within emerging economies where large segments of the population are under-banked.

It is assumed that in most countries where USAID operates, the current infrastructure and technology adoption is better suited to remote payments than it is to proximity payments. However, this document provides a brief description of proximity payments as their use is growing at a rapid rate within developed markets and because NFC presents a leapfrog opportunity for emerging markets where credit/debit card use is limited – as has been evidenced by the launch of a Google wallet in the U.S. in 2011<sup>25</sup> and NFC based transit

---

<sup>23</sup> Dodd-Frank Wall Street Reform and Consumer Protection Act , Pub.L. 111-203, H.R. 4173

<sup>24</sup> OCC Bulletin 2006-34

<sup>25</sup> Google, Citi, MasterCard, First Data and Sprint Team up to Make Your Phone Your Wallet” at: [http://www.google.com/press/pressrel/20110526\\_wallet.html](http://www.google.com/press/pressrel/20110526_wallet.html)

products such as the Oyster card in London,<sup>26</sup> and the increasing prevalence of NFC-based payment technology in Asian markets.

### 4.2.1. Description: Mobile Remote Payments

Remote payments do not require the user to be in the vicinity of a card reader to conduct a transaction. There are several technologies that enable remote payments, including browser-based, native payment applications, bill to carrier, and messaging-based.

The **Messaging-based approach** uses either the Short Message Service (SMS) or Unstructured Supplementary Service Data (USSD) to initiate or authorize a payment transaction. At the time of writing, SMS and USSD are the predominant technologies used for enabling mobile payments in many of the countries within which USAID operates. Our subsequent review is focused on mobile payments enabled through SMS and USSD and provides detailed information on viable models.

**Browser-based technology**, also referred to as WAP enabled websites, replicates an e-commerce environment on a mobile device. Due to the constraints of the device, mobile optimized websites typically adapt site functionality to suit the specifications and user experience of a mobile device. Transactions are completed via the website but it is accessed from the mobile device. This assumes the payer has an acceptable method of payment to provide to the website.

**Native payment applications** are software that can be downloaded from an app store (such as the Android market place or Apple's App Store) and installed on a smartphone. These applications may provide an alternative way of accessing existing payment types, e.g. pre-paid cards that reside on a web server. An example is the Starbucks pre-paid payment app that can be downloaded from the app store. The consumer sets up his pre-paid card to provide the payment functionality that is accessed by the app. At the POS, a two dimensional bar code is generated on the phone that is presented to the cashier. The cashier scans the barcode which is transmitted to Starbucks' servers and which points to the user's account. The amount of the transaction is deducted from the pre-paid card and the transaction completed at the POS. Although it looks like a proximity payment it is in effect a remote payment.

The **bill to carrier approach** allows users to charge transactions to their mobile bill. This works against either a pre-paid plan or a post-paid plan. Due to the risk inherent for the MNOs they typically do not allow this to be used for higher ticket size transactions but rather limit it to low ticket size high margin transactions such as digital downloads or ring tones.

---

<sup>26</sup> Transport for London to accept NFC payments from 2012" at: <http://www.nfcworld.com/2011/07/12/38537/transport-for-london-to-accept-nfc-payments-from-2012/>

## Electronic and Mobile Payments: *Mobile Payments*

As the remote payments ecosystem is continuing to evolve and blurs traditional roles between MNOs, financial institutions, and agents in the payments lifecycle, Figure 7<sup>27</sup> provides a high-level overview to guide the reader.

**Figure 7: Mobile Payment Stakeholder Description**

Stakeholder	Assets / Capabilities	Incentives	Roles	Limitations / Constraints
<b>Mobile Network Operators</b>	<ul style="list-style-type: none"> <li>• Mobile Infrastructure</li> <li>• Retail outlet / agent network</li> <li>• Branding</li> <li>• Customer service</li> </ul>	<ul style="list-style-type: none"> <li>• Acquire and retain customers</li> <li>• Manage churn</li> <li>• Increase revenue</li> <li>• Meet service obligations</li> </ul>	<ul style="list-style-type: none"> <li>• Provide infrastructure and communication service</li> </ul>	<ul style="list-style-type: none"> <li>• Regulation and policy may limit ability to provide financial services.</li> </ul>
<b>Banks</b>	<ul style="list-style-type: none"> <li>• Banking license</li> <li>• Infrastructure</li> <li>• Financial sector regulatory experience</li> <li>• Retail outlets</li> </ul>	<ul style="list-style-type: none"> <li>• Reduce cost of delivering services</li> <li>• Establish presence in new customer segments</li> </ul>	<ul style="list-style-type: none"> <li>• Offer banking services via mobile</li> <li>• Hold float in customer's names</li> <li>• Ensure compliance with financial sector regulations</li> <li>• Support settlement between mobile money issuers and agents</li> </ul>	<ul style="list-style-type: none"> <li>• Lack of experience with low-income customers</li> <li>• Stringent regulatory regimes</li> <li>• Present only in areas with dense populations</li> </ul>
<b>Agents</b>	<ul style="list-style-type: none"> <li>• Physical points of presence</li> <li>• Customer trust</li> <li>• Knowledge of customer usage habits and needs.</li> </ul>	<ul style="list-style-type: none"> <li>• Earn commissions on transactions</li> <li>• Increase traffic and sales potential.</li> </ul>	<ul style="list-style-type: none"> <li>• Perform cash-in cash-out transactions</li> <li>• Handle account opening procedures</li> <li>• Report suspicious transactions.</li> </ul>	<ul style="list-style-type: none"> <li>• Liquidity shortfalls</li> <li>• Limited ability to partner with larger corporations</li> <li>• Regulation and policy may limit services</li> </ul>

### Mobile Payment Operating Models

There are several operating models for mobile payments that are currently implemented in different markets. For the purposes of this report, we will follow the classification adopted by USAID in the Mobile Financial Services Risk Matrix, published by USAID in July 2011.

- **Bank Model** – In a pure bank model the bank (or other formal deposit taking institution) holds the license. Each client is required to have an established account with the bank.
- **MNO Model** – A pure MNO service extends the wireless network messaging functionality to provide payment services that enable customers to electronically remit funds to others on the same network. Electronic funds can then be converted to cash through the MNO's established agent network. Individual payment transactions occur entirely within the MNO and do not require the Payment Beneficiary to have a bank account.

<sup>27</sup> *Mobile Money Ecosystem Stakeholders (Adapted from: Developing mobile money ecosystems)*

## Electronic and Mobile Payments: *Mobile Payments*

- **Hybrid Models** – Hybrid models include but are not limited to:
  - MNO/Bank Model – Cell phone company-based payment services that handle payments internally with cash in/out through the MNO's agent network, yet link to formal banking by enabling communications with the bank and transfers between the user's cell phone payment account and accounts at the bank.
  - Government Provider/Bank Model – A government sponsored interbank clearing system includes consumer access functionality, either using smart cards or smart cell phone Sims that temporarily act as a store of value and synchronize with a formal bank account. The cell phone company, if involved, provides communications services while the government operates the payment switch between banks and between accounts within banks.<sup>28</sup>
  - Integrated Payments Provider Model – A payments company that is not bank owned or MNO affiliated and enables payment transactions leveraging a variety of tender types, from paper vouchers to mobile P2P payments and agent networks.<sup>29</sup>

Depending on the country USAID is operating within, the model used and the actors within the model may change. However, Figure 8 provides a generalized view of the roles and responsibilities within the most frequently used models.

Figure 8: Mobile Payment Models Roles and Responsibilities

Operating Model	Deposit Holder	Account Holder	Account set-up	Cash In	Cash Out	Transactions	Regulatory Framework
Bank	Bank	Individual	Customer identification performed in person by bank employees	ATM Agents Branches	ATM Agents Branches	Checks Credit cards Debit cards Pre-paid cards EFT Mobile P2P	1. Host country banking regulation 2. International regulation: AML, FATCA
MNO	Bank (Trust Account)	MNO	Customer identification performed in person by MNO employees or agents	Agents MNO Retail Outlets	Agents	Mobile P2P	Varies by country

<sup>28</sup> Mobile Financial Services Risk Matrix, Page 3. July 2010

<sup>29</sup> A prime example is Zambia's Mobile Transactions that has built a proprietary switch and its own distribution network, connecting MNOs, FIs and NGOs in country; go to: [www.mtzl.net](http://www.mtzl.net)

## Electronic and Mobile Payments: *Mobile Payments*

Operating Model	Deposit Holder	Account Holder	Account set-up	Cash In	Cash Out	Transactions	Regulatory Framework
Hybrid MNO - Bank	Bank (Trust Account)	MNO	Customer identification performed in person by bank employees	ATM Agents Branches MNO Retail Outlets	ATM Agents Branches	Checks Credit cards Debit cards Pre-paid cards EFT Mobile P2P	1. Host country banking regulation 2. International regulation: AML, FATCA
Hybrid Government-Bank	Bank	Individual	Customer identification performed in person by government or bank employees	ATM Agents Branches	ATM Agents Branches	Checks Credit cards Debit cards Pre-paid cards EFT Mobile P2P	1. Host country banking regulation 2. International regulation: AML, FATCA
Integrated Payments Provider	Bank (Trust Account)	Individual	Customer identification performed in person by payments provider employees or agents	Agents	Agents	Checks Credit cards Debit cards Pre-paid cards EFT Mobile P2P	1. Host country banking regulation 2. International regulation: AML, FATCA

### 4.2.2. Uses, Limitations, Risks, and Mitigants: Mobile Remote Payments

The mobile remote payment type offers USAID Missions or Implementing Partners an alternative to cash disbursements to Payment Beneficiaries. Depending upon the specific implementation or availability of remote payment method, this particular payment type is often best suited for use within the developing world. For example, with the significant amount of existing and stable infrastructure to support messaging-based remote payments, there are often very low barriers to entry for adoption. However, as with any technological or process advancement there are use cases, limitations, risks, and potential mitigants that must be considered prior to making a decision.

#### Uses for Mobile Remote Payments

- **Person to Person Payments** – Remote mobile payments transacted via messaging services can effectively execute P2P payments. Assuming both parties possess a mobile phone, Payment Beneficiaries can execute transactions to purchase goods and services, and send money to other people.
- **Entity to Person Payments** – Remote mobile payments can be used by entities such as governments, businesses, or non-profit organizations to execute a payment to an individual who possesses a viable mobile phone and account.



## Electronic and Mobile Payments: *Mobile Payments*

- **Person to Entity Payments** – Remote mobile payments can be used for bill or tax payments to a private business or government entity.
- **Internet transactions** - Remote mobile payments can be used to complete internet transactions via websites or through native applications.

### Limitations of Mobile Remote Payments

- **Cash Access** – Currently there are no technologies that support the use of a remote payment device to receive cash without converting the digital payment to physical cash through an agent or secondary device.
- **Infrastructure** – Network coverage is required for Payment Beneficiaries to execute transactions using a mobile device. In some environments, this may be limited to a specific MNO network, as not all MNOs in a given country may offer mobile payments services. This could be a significant inhibitor in rural areas where appropriate network coverage is not yet available or is unreliable or when the mobile payment services are offered by a single MNO

### Risks for Mobile Remote Payments

- **Technology (Software)** – Remote payments rely on software either installed (smart phone applications) or resident (software enabling text messaging) on a device. These applications are susceptible to cyber-crime and can pose a security risk.
- **Technology (Hardware)** – Though account information is typically stored in the cloud for mobile remote payments (rather than on the phone itself), this hardware failure could significantly impact Payment Beneficiaries' access to funds.
- **Infrastructure** – Network systems must exchange confidential information to complete a transaction. This can be susceptible to cyber-crime and can pose a security risk. In addition, network failure or government infrastructure failure (e.g., power outage) can result in a significant reduction in payment execution capability.
- **User Anonymity** – Anonymous usage is more common and easier to accomplish with mobile remote payments than with other electronic forms of payment (including EFT, some forms of pre-paid cards, and mobile proximity payments). This anonymity presents opportunity for money laundering and other forms of fraud.
- **Network Interoperability** – Many providers of mobile remote payments services operate solely (or at least with the least difficulty) within a single MNO network. This can prevent risk that Payment Beneficiaries will have difficulty receiving or using funds in areas where multiple providers exist.

### Mitigation Strategies for Mobile Remote Payments

- Native applications, if used to facilitate mobile remote payments, should be built by experienced mobile developers and tested exhaustively prior to deployment with reference and adherence to current industry standards if available or applicable.

## Electronic and Mobile Payments: *Mobile Payments*

- Native applications should avoid caching data where possible.
- A “kill switch” can be built into the app or other payment platform such as software enabled SMS or USSD platforms where the access is denied to the consumer if the app or system has been found to contain vulnerabilities.
- Mobile service providers should maintain extensive business continuity plans that enable continued service through disaster situations that can result in service interruption or network outages. These plans could include building in network redundancy, providing back up power sources for mobile base stations, and our network downtime protections.
- User education is an effective mitigant of cyber-crime, users can be educated on best practices for information security including: PIN guarding, regular password changes, and device guarding.
- Twenty-four hour user support services provide an effective second line defense that allows users to report and disable compromised accounts.

### **4.2.3. Regulation: Mobile Remote Payments**

The regulation and guidelines for remote mobile payments is determined on a country specific basis. While some countries have begun to set the standard for adaptation of financial entity regulations to account for the emergence of remote mobile payments models, there are no agreed upon standards and country-level adoption is inconsistent – particularly in developing economies.<sup>30</sup> As the mobile payments industry continues to evolve, standards may emerge that, if followed, should be evaluated for their impact on the risk of mobile payments. Depending on the framework, regulations that are prohibitive or overly restrictive also may impede the offering of mobile payment systems, making them unavailable or limited in a given local country context.

### **4.2.4. Description: Mobile Proximity Payments**

Proximity payments make use of NFC technology. NFC is a short range high frequency wireless communication technology, typically presented on a chip that enables an exchange of data between an initiator and a target. Chips can be embedded in cards, presented as a key fob or integrated in mobile devices. The target, e.g. a card reader, needs to have the required hardware and software components to accept these communications.

NFC leverages existing contactless payment standards based on the EMV smartcard protocol that has been rolled out across markets globally and currently represents the most secure card technology in wide use. The chip enables dynamic authentication and has been a proven tool in fraud reduction. Mobile applications that leverage NFC for communicating with a card reader must address the security of user credentials. This is done in Secure Element – a platform on the device that can be housed on the subscriber

---

<sup>30</sup> Best Practices for Mobile Device Banking Security 2008, ATM Industry Association, pg 57

## Electronic and Mobile Payments: *Mobile Payments*

identity module (SIM) card or on a separate secure digital (SD) card. The underlying payment instrument can be a debit card, pre-paid card or credit card. Proximity payments therefore represent a new access tool for existing card products. However, the set-up of a digital wallet requires extra steps and adds a new dimension to this product.

### Account set-up

- Mobile payment applications can be downloaded to the mobile device by the manufacturer or by the end user.
- The provisioning of credentials typically takes place over the air (OTA). In a typical case the user will have set up the account on the Web and will then access that information to supply the credentials in his wallet.
- The user's credentials are stored in the "Secure Element" of the device and communication between application and secure element is provided by the Trusted Service Manager (TSM) module.

### Transaction flows:

The transaction flows are identical to those of a regular card transaction as the telephone is substituted for the plastic – and the terminal upgraded – and there is a change in form factor but not in process.

#### **4.2.5. Uses, Limitations, Risks, and Mitigants: Mobile Proximity Payments**

The mobile proximity payment type offers USAID Missions or Implementing Partners an alternative to cash disbursements to Payment Beneficiaries. However, as with any technological or process advancement there are use cases, limitations, risks, and potential mitigants that must be considered prior to making a decision.

### Uses for Mobile Proximity Payments

- **Point of Sale Transactions** – Proximity payments are well suited for POS transactions. While there is a notable limitation that a vendor or merchant must have POS infrastructure in place, a proximity payment allows for convenient as well as electronically traceable transactions.

### Limitations of Mobile Proximity Payments

- **Non Face to Face Transactions** – Due to the physical nature of proximity payments, they are not viable for transactions that do not require an-in person interaction. By definition, "proximity" restricts transaction types to those that can be accomplished with both parties near one another.
- **Person to Person Payments** – Currently, P2P proximity payments require both payer and payee to have NFC enabled devices. In most cases, a proximity payment

## Electronic and Mobile Payments: *Mobile Payments*

uses a device on the payer side of the transaction that communicates with a POS device on the recipient side of the transaction.

- **Cash Access** – Currently there are no technologies that support the use of a proximity payment device to receive cash other than receiving a “cash out” at a retailer that is equipped with a proximity POS device.
- **Point of Sale Devices** – In order for Payment Beneficiaries to spend the funds available via the proximity payment device, merchants and/or vendors must have matching POS devices.

### Risks for Mobile Proximity Payments

- **Application Design** – Many proximity payments rely on software either installed or resident on a device. While the chipsets powering these devices adhere to proven standards, the applications themselves may pose security risks. For example, Via Forensics’ App Watchdog has performed tests on the first digital wallet that was broadly rolled out in the U.S. (the Google wallet) and identified a number of risks including the risk of third parties capturing customer data stored in a mobile user’s Google wallet. The risks are in the design of the mobile or digital wallet application and not in the chip technology which is a proven standard. Via Forensics addressed their warning to banks issuing digital wallets for download and use as proximity payments.<sup>31</sup>

### Mitigation Strategies for Mobile Proximity Payments

- Wallet applications should be built by experienced mobile developers and tested exhaustively, prior to deployment with reference and adherence to current industry standards if available or applicable.
- Wallet applications should avoid caching data where possible.
- A “kill switch” can be built into the app where the access is denied to the consumer if the app has been found to contain vulnerabilities.

#### **4.2.6. Regulation: Mobile Proximity Payments**

There are currently no regulations or guidelines specific to proximity payments as they merely add a new form factor to an existing payment system, namely the four party credit card or debit card system. All regulations and guidelines applicable to the underlying instruments, debit/credit/pre-paid cards, applies. However, there are industry standards for the chip protocol and there have been recent industry announcements of the creation of new consortia or joint ventures to define standards for securing transactions.<sup>32</sup>

---

<sup>31</sup> Mobile App Security and Payments. ViaForensics. Presented at 2012 Payments Forum.

<sup>32</sup> ARM, Gemalto and Giesecke & Devrient Form Joint Venture to Deliver Next-Generation Security for Services Running on Connected Devices “, April 3, 2012, as published on:  
<http://www.businesswire.com/news/home/20120402006967/en/ARM-Gemalto-Giesecke-Devrient-Form-Joint-Venture>

## 5. RISK ANALYSIS AND MITIGATION

The risk profile for an individual USAID Mission or program with regard to funds disbursement is highly variable, making the development of standard policies or guidelines a challenge for the Agency. For this reason, the following section provides a framework for assessing risk across all payment options, as well as detailed descriptions of each risk type with relevant mitigation strategies. This establishes a baseline understanding of the risk landscape that can be referenced when evaluating payment options.

Risk definitions are based on the USAID Mobile Financial Services Risk Matrix developed in July 2010.<sup>33</sup> Risk categories have been consolidated and summarized for the purpose of this report. Additional risks and categories have been added to the analysis by the authors of this document. Figure 9, below, provides a high-level definition for the risk categories evaluated.

Figure 9: Risk Descriptions

Risk	Description
Financial	Risk of a single transaction failure in which the intended Payment Beneficiary receives fewer funds than expected, or does not receive payment at all
Systemic	Risk of collapse of a financial system or market
Legal	Risk which could result in lawsuits, judgment or contracts that could disrupt or affect business practices. AML/CFT vulnerability is the most significant legal risk in this context
Operational - General	Risk which damages the ability of one of the payment stakeholders to effectively operate their business, results in a direct or indirect loss from failed internal processes, people, systems or external events
Operational - Interoperability	Risk that the lack of inter or intra network operability may prevent a consumer from transacting successfully with the desired party
Operational— Customer ID and Authentication	Risk that a transaction fails or that funds do not reach the Payment Beneficiary due to inability to verify the validity of transfer parties
Operational— Provider Governance	Risks to customer funds that arise out of a lack of appropriate governance structure, standards and practices
Technology	Risk that technology failure will result in a direct or indirect loss to a stakeholder in the payment process
Reputational	Risk that damages the image of one of the stakeholders, the mobile system, the financial system, or of a specific product

The following sections further define each risk category and summarize the risks encountered by stakeholders in the context of each payment type. Figure 10 provides a summary overview of the risk burden for each payment type, as well as the types of mitigations recommended.

<sup>33</sup> Mobile Financial Services Risk Matrix July 2010

# Risk Analysis and Mitigation: *Financial Risk*

Figure 10: Risk Assessment and Mitigation Summary

Risk		Cash	EFT	Pre-paid Cards	Mobile
Financial	Risk	High	Low	Moderate	Moderate
	Mitigation <sup>34</sup>	Other	Reg/IC/Other	Reg/IC/Other	Reg/IC/Other
Systemic	Risk	N/A	Low / Moderate	Low	Low
	Mitigation	N/A	Reg/IC/Other	Reg/IC/Other	Reg/IC/Other
Legal	Risk	High	Low	High	High
	Mitigation	Reg/IC	Reg/IC/Other	Reg/IC/Other	Reg/IC/Other
Operational – General	Risk	Moderate/High	Moderate	N/A	N/A
	Mitigation	Other	IC/Other	N/A	N/A
Operational Interoperability	Risk	N/A	N/A	Low / Moderate	Moderate
	Mitigation	N/A	N/A	Reg/Other	Reg/Other
Operational Customer ID and Authentication	Risk	N/A	N/A	High	High
	Mitigation	N/A	N/A	Reg/IC/Other	Reg/IC/Other
Operational – Provider Governance	Risk	N/A	N/A	Moderate	Moderate
	Mitigation	N/A	N/A	Reg	Reg
Technology	Risk	N/A	Low	Moderate	High
	Mitigation	N/A	Reg/IC/Other	Reg/IC/Other	Reg/IC/Other
Reputational	Risk	Moderate	Low	Moderate	Moderate
	Mitigation	Other	Other	Other	Other

## 5.1. Financial Risk

Financial risk can be summarized as the likelihood of a single payment transaction failing in some way. More specifically, it is the risk that the Payment Beneficiaries receives fewer funds than the sender intended, or that the funds never reach the intended recipient. Financial risk typically occurs as a result of the following three circumstances:

- Non-transparent or variable transaction costs
- Fraud
- Theft

Transactions costs are fees or administrative costs, for which the sender and/or recipient may be responsible, associated with execution payment transactions. These costs should not uniformly be considered a financial risk, as in many cases, they are able to be accurately estimated in advance of selecting a payment type. However, in some cases transactions costs may not be made transparent by the provider, or may be variable based on future environmental circumstances. In this manner, non-transparent or variable

<sup>34</sup> **Reg:** Regulatory  
**IC:** Internal Controls  
**IS:** Industry Standards  
**Other:** Variable or informal process-related

## Risk Analysis and Mitigation: *Financial Risk*

transaction costs should be considered as a financial risk.

Fraud is defined as either criminal or wrongful deceit, with the intention to financially benefit. This risk is presumably able to be mitigated through customer authentication and authorization but should be understood as a component of overall risk.

Theft is inherent in the physical nature of cash. The transport required for physical currency creates a theft risk. Unlike transactions processed via an electronic network, cash requires transport and transfer of a physical currency with no ownership restrictions and other than possession.

### 5.1.1. Cash Payments

Transaction costs for cash include fees, personnel and equipment costs associated with the acquisition, transportation, protection/security, or disbursement of physical currency. In some environments, it may be possible to estimate these costs in advance, but there is typically some risk that they will be higher than expected. Programs in an environment of intermittent or ongoing conflict may experience fluctuations in the amount of security required, for example.

An example of cash transaction costs comes from an Implementing Partner supporting a USAID civil society strengthening program in Kenya who reported that, including salaries, transportation, fuel and other costs, the total transaction cost associated with paying cash for a single training workshop was Ks 46,500, or almost \$560. In this case, because security was not a major issue, it may have been possible for the Implementing Partner to anticipate those costs, thus minimizing transaction cost risk. However, a similar program in Afghanistan would need to consider the risk that these costs would increase in times of elevated conflict. This could possibly be contrasted with other payment types. For instance, when the program in Kenya adopted mobile

#### Process Requirements for Cash Payments

- The Area Supervisor collects and verifies attendance lists with each Site Supervisor.
- The Area Supervisor works with finance staff to prepare payment vouchers and bank transfer requests (as appropriate), indicating days/ hours worked and total payments per work group.
- On payday, the Area Supervisor visits the worksite with attendance lists and explains the payment process together with the Site Supervisor.
- All beneficiaries present identification or, if identification does not exist, a Group Leader or community representative who knows the participants must be present to verify identities.
- Literate beneficiaries should be enlisted to assist others.
- Beneficiaries receive the exact amount due and sign the cash payment sheet (Annex 13) on receipt or put a thumbprint next to their name in recognition of received payment.
- All payments sheets must be countersigned.
- Payment vouchers and attendance lists are re-tabulated and reconciled by Finance Officers.

- *MercyCorps Guide to Cash-for-Work Programming*

## Risk Analysis and Mitigation: *Financial Risk*

payments through M-Pesa, total transaction costs were reduced to Ks 3,750, or \$35.<sup>35</sup> More importantly, those transaction fees are much less variable based on environmental conditions. A recent study commissioned by CALP, the Cash Learning Partnership, found that “the emerging evidence suggests that there may be cost savings in switching to new technologies, especially over a longer time horizon.”<sup>36</sup>

Cash transaction fraud occurs in two primary ways. The most common is through graft and corruption. Government officials, payment intermediaries or some other actor in the cash transaction intercept cash payments or misrepresent the Payment Beneficiary. As a result, funds are not applied as expected and transaction costs for people and businesses are increased. In many cases of graft and corruption with cash transactions, the payment provider is unaware that fraud has occurred, making it difficult to determine the full extent of fraud impact.

The second form of cash transaction fraud is the distribution and use of counterfeit currency. In this circumstance, an actor in the process of supplying physical currency for the payment of Payment Beneficiaries substitutes counterfeit currency for legitimate funds. In the case of counterfeiting, fraud is more often detected.

The transport required for physical currency creates a theft risk. Unlike transactions processed via an electronic network, cash requires transport and transfer of a physical currency with no ownership restrictions other than possession. In violent or conflict-prone geographies, the known distribution of cash can increase the financial risk to the Payment Beneficiary as well as create a physical threat. An example of how this impacts citizens in Haiti and the potential for improvement was provided by the authors of a recent study on Haiti. “Bianca, a vendor who sells vegetables on Route Delmas and a TchoTcho customer, told us that an advantage of mobile money is that she can deposit her day’s wages at an agent near her stall and withdraw at an agent in her neighborhood. Bianca thereby avoids the stress of travelling with money and the possibility of being robbed as she travels home. She says that she would rather pay the cost of withdrawing money than risk losing everything.”<sup>37</sup> However, this can create the unique risk of relying on agents, rather than bank branches, to manage cash payments. These agents, who need to maintain liquidity for mobile money transactions then become known as a habitual carriers of cash. This can have the dangerous effect of increasing risk of theft rather than decreasing it, in some environments.

### *Financial Risk Mitigation – Cash Payments*

Mitigation of financial risk for cash transactions is often managed through adoption of strong internal controls and audits by donor organizations and Implementing Partners.

---

<sup>35</sup> It’s Better Than Cash: Kenya Mobile Money Market Assessment; Loretta Michaels; USAID, p. 32

<sup>36</sup> New technologies in cash transfer Programming and Humanitarian Assistance, CALP, page 46

<sup>37</sup> “Mobile Money in Haiti: Potentials and Challenges”. Institute for Money, Technology and Financial Inclusion April 2011, page 7



## Risk Analysis and Mitigation: *Financial Risk*

Specific controls are put in place to:

1. Limit cash access. Implement specific procedures to define who has access to cash and the manner in which cash movements are executed. Vary transport routes and distribution centers or timing and use cash transport companies (i.e. armored cars).
2. Impose tracking requirements. Implement policies on receipt requirements for cash disbursements.
3. Conduct regular reconciliations. Require to validation of receipts against approved expenses and cash stores.

The MercyCorps Guide to Cash-for-Work Programming (described above) provides a thorough example of detailed internal controls and processes to mitigate financial risks related to cash transactions.

It should also be noted that the adoption of a more secure and transparent payment type as an alternative to cash is a reliable method for mitigating financial risk. This will be discussed in greater detail later in this document.

### **5.1.2. Electronic Funds Transfer**

Transaction costs for EFT are typically a straightforward fixed fee per transaction. Payment recipients' banks will often charge a fee to receive the funds and to disburse them to the Payment Beneficiary. Because such fees are almost universally transparent, transaction costs are not really a financial risk factor for EFT.

In addition, EFT is typically done through the SWIFT system, a high standardized, global system that has established policies and procedures. As with any system requiring human input, EFT systems are susceptible to fraud from both employees and intruders. As instructions for wire transfers or ACH entries are processed by employees, there is the possibility of error or misdirection of the transfers to persons other than the intended recipients. Similarly, those with access to the systems executing the transactions can alter data to re-direct funds. This represents vulnerability in all environments where non secure devices, e.g. a computer connected to a server via the Internet, are used to carry out these processes.

The risk of fraud in EFT is inversely related to the rigor of the controls put in place, and to the degree of transparency with regard to the process actors. For this reason, intra-bank transfers are the form of EFT most susceptible to fraud. Intra-bank transfers are often used when the banking system in a given country is not mature enough to support consistent, reliable, and low cost inter-bank transfers.

#### *Financial Risk Mitigation – Electronic Funds Transfer*

Financial risk is already significantly lower for EFT payments than for any other payment

## Risk Analysis and Mitigation: *Financial Risk*

option. For this reason USAID leverages EFT for payment execution when it is an available option. Financial risk mitigation is best achieved through adoption of standard banking industry internal controls with regard to transaction tracking and monitoring, redundant roles and responsibilities and regular internal audits.

### **5.1.3. Pre-paid Cards**

Pre-paid cards can carry both costs to the consumer and to the merchant where cards are used. In situations where cards are loaded by one funding entity to benefit many (e.g. disbursement of monthly benefits) there may also be fees and charges to the funding entity. Costs to the consumer associated with pre-paid cards fall into three categories:

- Load fees for adding funds to the account either at account opening or subsequently
- Usage charges for purchases, bill payment and cash withdrawals
- Service fees, e.g. for balance inquiries or paper statements

These fees are almost usually transparent – at least when the pre-paid card provider is an established global credit card company and the payment type is a simple pre-paid debit card. As such, this is not really a financial risk, but more of a financial consideration.

The fees are often designed to drive consumer behavior that minimizes costs to the bank by pushing them to the purchasing entity or to the merchant at the transaction level. This may reduce the utility of pre-paid cards to some Payment Beneficiaries, making transaction costs an important consideration.

The two major fraud categories perpetrated on credit, debit and pre-paid cards are internal and external fraud. Internal fraud typically takes the form of data breaches where payment service company employees provide criminals access to accounts through stolen credentials. While these types of attacks are infrequent, they can result in millions of cards being exposed and occur in any geography, including both the U.S. and emerging markets.

External fraud is typically due to customer loss of a card or capture of a customer's card information by a merchant or other third party. External fraud can also arise from a card processing failure. This can create exposure to the possibility of card counterfeiting during the process of personalization, during transactions or at the various locations pre-paid cards need to be stocked before delivery to the recipient. In each of these cases, information is stolen at points in the payment process and used to wrongly disburse or use funds.

#### *Financial Risk Mitigation – Pre-paid Cards*

Regulation and standards are one of the mitigants for high transaction costs being charged to consumers. In terms of fees being charged to single funding units such as a government agency, a competitive Request for Proposal (RFP) process will generate lower fees and also

## Risk Analysis and Mitigation: *Financial Risk*

allow the funding agency to negotiate terms for the consumer usage.

Fraud as defined above is typically an outcome of a failure to develop appropriate processes and controls. In the section on operational risks and technology risks, we discuss a number of mitigants that can mitigate fraud risk. At a high level these are:

- Processes to properly authenticate customers at the point of interaction
- Internal controls to prevent internal fraud
- Payment card industry data security standards (PCI DSS)<sup>38</sup>
- Ability to trace use and reject card authentication remotely

### 5.1.4. Mobile Payments

There has yet to emerge a clear standard for transaction costs associated with mobile money given the variety of business models for delivering such services, however current trends from influential mobile payments providers point toward full transparency, which likely means that undisclosed transaction fees are not a notable financial risk factor for mobile payments. The transaction fee rate card for M-Pesa, which is seen as a leading mobile money provider in terms of adoption, can serve as a notable example. M-Pesa have a tiered fee per transaction pricing structure, for which the sender is responsible.

M-Pesa transaction costs fall into several categories and are listed here in Kenyan Shilling (85 KSH = \$1.00 as of May 2012).

Figure 11: M-Pesa Tariff Example<sup>39</sup>

Transaction Type	Cost (KSH)	Cost (\$)	Tiers
Deposit cash	KSH 0	\$0.00	
Send money to registered user	Flat 30 KSH	Flat \$0.36	
Send money to non - registered user	Tiered KSH 75-400	Tiered \$0.90 - \$4.80	(1.14% to 3.00%)
Withdrawal reg. user at registered outlet	Tiered KSH 25-170	Tiered \$0.30 - \$2.40	(0.49% to 1.00%)
Withdrawal reg. user at PESA Point ATM	Tiered KSH 30-175	Tiered \$0.36 - \$2.10	(0.88% to 1.20%)
Withdrawal by non-registered user	KSH 0	\$0.00	
Bill pay transaction	KSH 0-30	\$0.00 - \$0.36	

Mobile payments are inherently network-based, interfacing with the mobile device's platform to authenticate and process transactions. Account registration and device recognition are used to support transaction accuracy. As with other network-based

<sup>38</sup> Payment Card Industry Data Security Standard (PCI DSS) is an [information security](#) standard for organizations that handle cardholder information for the major [debit](#), [credit](#), [pre-paid](#), [e-purse](#), [ATM](#), and [POS](#) cards.

<sup>39</sup> [http://www.safaricom.co.ke/fileadmin/M-PESA/Documents/MPESA\\_TARRIF.pdf](http://www.safaricom.co.ke/fileadmin/M-PESA/Documents/MPESA_TARRIF.pdf)

## Risk Analysis and Mitigation: *Financial Risk*

payment systems, fraud is possible through wrongful acquisition of mobile account information. To date, there is no reliable data on mobile payments fraud. There have been no widespread reports of fraud in mobile money systems and trust is identified as one element of adoption and uptake of mobile money platforms.

However, in a recently reported fraud case involving mobile money in Uganda, the perpetrators executed a classic internal fraud scheme and unlawfully transferred funds from victims' accounts using stolen access credentials.<sup>40</sup> Fraud at an individual customer level, in which a customer's credentials are stolen, will be described in more detail in the section on operational risk. Fraud linked to the device will be covered in more detail in the section on technology risks.

### *Financial Risk Mitigation – Mobile Payments*

Regulation, standards and market competition are the best methods for driving down transaction fees, so encouragement of such a competitive environment is a long term mitigation strategy. In the immediate term, it is generally challenging to negotiate lower transaction fees on behalf of consumers when emerging players are still in the development phase and need to charge higher fees before they reach scale in their operations. It may also be the case, those disbursing funds to Payment Beneficiaries may elect to absorb the transaction fees as part of programming costs reducing the risk to the Payment Beneficiary. Transaction fees may apply to transactions following disbursement, such as cash-out withdrawals or purchase of goods, which may impose a cost on the Payment Beneficiary not typically associated with cash.

Mitigants for general fraud risk associated with mobile payments are similar to those of EFT payments and pre-paid cards. Strong regulation or standards and robust internal controls allow for mitigation of general fraud risk. The ability to track mobile payments by location and the creation of a digital transaction footprint provide a means by which potentially fraudulent activity can be discovered, investigated and potentially prevented. More specific mitigants, such as two-factor authentication for individual customer-level fraud, are described in more detail in the section on Operational Risks. Mitigants for fraud linked to the device are covered in more detail in the section on Technology Risks.

#### **5.1.5. Relevance to USAID and Implementing Partners**

Mitigating financial risk as described within this section, is directly related to the delivery of effective foreign aid. As financial risk increases the possibility of Payment Beneficiaries either not receiving or being defrauded of intended funds, this category of risk is of the utmost importance. While it is not possible to wholly eliminate financial risk, there are steps USAID Missions or Implementing Partners can take to make informed decisions with respect to payment type options.

---

<sup>40</sup> <http://mobilemoneyafrica.com/mtn-uganda-loses-billions-to-mobile-money-fraud-involving-employees/>

## Risk Analysis and Mitigation: *Systemic* Risk

EFT at both the inter- and intra-bank level is the least susceptible to financial risk where there is reasonably high trust in the viability and maturity of the banking industry as well as a high percentage of banked Payment Beneficiaries. Where EFT is not possible, electronic or mobile payments providers have demonstrated the capability of providing similar protections against financial risk – particularly fraud and theft – when proper controls are in place. These factors must be considered by USAID and Implementing Partners when evaluating these payment types in a specific country context.

Despite these options, there are circumstances where cash is the only viable option. If identified Payment Beneficiaries are unbanked and mobile money or pre-paid card providers are unavailable - or if pre-paid cards and mobile money present total transaction costs that make them undesirable options in comparison to cash – payers may determine the best method to mitigate financial risk is to use cash payments.

USAID can play a role in the development of a mobile money ecosystem that serves consumer needs by encouraging Implementing Partners to work with MNOs and banks that have appropriate fraud controls in place. In order to accurately make decisions with respect to a payment type, USAID Missions or Implementing Partners must understand financial risk specific to their unique environment.

### 5.2. Systemic Risk

Systemic risk is defined as “A risk that could cause collapse of, or significant damage to, the financial system or a risk which results in adverse public perception, possibly leading to lack of confidence and worst case scenario, a ‘run’ on the system.”<sup>41</sup> This type of risk is not unique to developing markets, and may occur in any financial system.

More simply, systemic risk is the risk of collapse of a financial system or market, as opposed to risk associated with any one individual entity, group or component of a system. In selecting a payment method for disbursement of funds to Payment Beneficiaries, an Implementing Partner and USAID must consider the implications of payment failure on the stability of the overall system. For example, if an audit revealed that 25% of Payment Beneficiary payments made on a given contract were misappropriated for the purpose of money laundering or graft, would that destabilize the entire payment system?

A number of sub-risks fall into the category of systemic risk. Summarized below, the major systemic risks comprise:

- Government actions that hinder the organic development of a payment ecosystem.
  - Taxation – The government decides to tax transactions to generate governmental revenue, thereby increasing the marginal cost of each

---

<sup>41</sup> USAID Mobile Financial Services Risk matrix, page 3

## Risk Analysis and Mitigation: *Systemic Risk*

transaction beyond those deemed tolerable and limiting market growth.

- Market intervention – The government mandates use of a particular model, thereby constraining innovation, potentially reducing opportunity for competition, and hedging the success of the market on a single point of failure.
- Excess Regulation – The government imposes regulation that makes a payment system business model non-viable. Examples may include setting maximum transaction fees that are too low to allow for full cost recovery or mandating overly strict controls that make it impossible providers to comply.
- The growth of financial systems outside of the traditional bank model, particularly in a developing economy with an immature banking system, could slow maturation of the overall financial system of the country if these new systems draw customers away from the formal banking sector.
- Absence of government actions necessary to create a framework for a stable payments market. The lack of rules, regulations or standards that ensure a stable and compliant operation of payment providers expose the financial system to risks. In addition, regulatory uncertainty over the treatment of different payment methods can inhibit market entry or growth. This can undermine trust in the payment provider and the financial system and cause the system to fail.
- Absence of government supervision. If national regulators are unable to effectively investigate fraud or criminal activity due to lack of operational support systems and human capacity, regulations intended to protect consumers and the financial system will go unsupervised.

### **5.2.1. Cash Payments**

The implications of payment failure for cash are quite different than for payment methods that rely on larger payment systems. Cash payments, by their nature, are treated as individual transactions and not necessarily as part of a payment system. The failure of a single cash payment does not necessarily imply anything, in terms of risk, on future cash payments to another Payment Beneficiary or vendor. An instance of fraud or theft is unlikely to cast doubt on the entire system of currency. For this reason, systemic risk for cash payments is very low and somewhat irrelevant, even though financial risk – the risk of a single instance of fraud - is generally higher.

It should be noted that the application of systemic risk to cash payments precludes the collapse of country's native currency. While currency failure is indeed a systemic risk, the term "cash" applies to all possible physical currencies. Thus, in the event of a currency failure, another country's currency could supplant the failed native instrument.

#### *Systemic Risk Mitigation – Cash Payments*

Though currency is vulnerable to general systemic risk associated with currency stability (inflation, devaluation, etc.) these issues are likely to affect all payment types. As such, no

specific systemic risk mitigations for cash are necessary.

### **5.2.2. Electronic Funds Transfer**

For EFT, the implications of a single payment failure are significant. For example, if one out of every four EFT payments fails or is untraceable, it could potentially cast doubt on the security of the bank or the entire banking system in that country. These circumstances are far less likely for EFT than for cash, of course, as EFT payments are designed to maximize the traceability of transactions. Therefore, systemic risk is more relevant to EFT payments than to cash payments, but the circumstances that generate systemic instability are uncommon and at low risk of occurring.

#### *Systemic Risk Mitigation – Electronic Funds Transfer*

The mitigation for systemic risk related to EFT is similar to the mitigation for financial risk. Proper regulation of the banking system, insurance of bank transactions and transparency and accountability in funds management all contribute to overall trust and stability of the banking system

### **5.2.3. Pre-paid Cards**

The implications of payment failure for pre-paid cards vary, based on the location of the failure. As pre-paid cards operate on existing card processing infrastructure, the failure of a MasterCard instrument may not necessarily induce a failure of a VISA instrument. Essentially, pre-paid cards do not necessarily represent a single system, and thus are not completely susceptible to a perceived total failure of the payment type. Additionally, the processing networks for pre-paid cards are built to serve global needs, providing redundancy and monitoring capabilities. However, if a USAID Mission or Implementing Partner chooses a specific pre-paid card provider to execute all transactions, it may be the case that a failure of a payment casts doubts on the provider-specific system.

### **5.2.4. Mobile Payments**

Similar to pre-paid cards, the mobile payment type may not represent a complete or single system. In addition to the possibility of multiple providers, this issue is further compounded by multiple methods for executing a mobile payment. For example, a payment failure using a messaging-based approach may not necessarily cast doubt upon a proximity payment provider. This separation of mobile payment failure from the larger financial system of the country does present unique risks. While most governments provide some level of insurance on bank deposits there is generally no such standard requiring insurance for deposits in mobile banking systems. If a mobile payment provider collapses, user funds may be at increased risk.

However, as MNOs were originally positioned to serve customers with high network usage

## Risk Analysis and Mitigation: *Systemic Risk*

needs, most MNOs are vigilant with the monitoring and real time operations of their networks. The 24/7 nature of the mobile phone business tends to provide faster resolution times with respect to system outages as well as proactive avoidance of failures.

### *Systemic Risk Mitigation – Pre-paid Cards and Mobile Payments*

The mitigations for systemic risk with regard to electronic and mobile payments are quite similar, and also related to regulation and payment system oversight.

*The role of government in developing mobile money ecosystems cannot be overstated. Government regulators are responsible for providing environments that enable ecosystem development to happen. Regulators can create the space for experimentation and, as experience accumulates, build the policy frameworks needed to undergird further growth. This is, of course, not an easy exercise, with disparate and sometimes competing objectives that need to be reconciled.*<sup>42</sup>

At the same time that governments are looking to create or increase regulation or guidelines for electronic and mobile payments, they also recognize the benefits provided by alternatives to a bank-based financial system for increasing financial inclusion. In countries where the majority of the population is unbanked or under-banked and an equal percentage is equipped with mobile phones, there is a tremendous opportunity to bring more citizens into the financial system. Additionally, decreasing cash transactions generally increases the ability of the government to track and regulate payments.

Finding this balance and determining the right degree of legislative or supervisory government involvement is the major challenge in developing a viable framework for regulating electronic and mobile forms of payment.

Understanding that payment systems oversight is the best mitigation of systemic risk for electronic and mobile payments, the G20 has adopted regulatory guidelines that will support the effort to increase financial inclusion through regulation. Full details can be found in Appendix A, but it can be summarized by the following:

*Innovative financial inclusion means improving access to financial services for poor people through the safe and sound spread of new approaches. The (following) principles aim to help create an enabling policy and regulatory environment for innovative financial inclusion. The enabling environment will critically determine the speed at which the financial services access gap will close for the more than two billion people currently excluded. These principles for innovative financial inclusion derive from the experiences and lessons learned from policymakers throughout the world, especially leaders from developing countries.*<sup>43</sup>

---

<sup>42</sup> Developing Mobile Money Ecosystems, Beth Jenkins

<sup>43</sup> FATF Guidance Anti-money laundering and terrorist financing measures and Financial Inclusion, page 54



## Risk Analysis and Mitigation: *Systemic Risk*

The intent of this effort by the G20 is to establish financial inclusion as a priority, and to support the efforts of local governments in establishing regulations for oversight of financial entities in a manner that supports this priority. The Philippines provide an excellent example of regulators specifically addressing the issue of mobile payments. While incorporating a number of the principles laid out by the G-20, the Philippine Central Bank (BSP) also provides legal certainty to an evolving market. These rules have been put into practice in the form of Circular 649 on the Issuance of Electronic Money by the BSP. On 26 February 2009, the BSP, with support from USAID, issued an ‘e-money’ circular that opens e-money issuance to non-banks. Such e-money regulation enables non-banks to offer electronic money solutions and e-money issuance is open to banks and non-banks under the same rules. The Circular was the result of a collaborative process between the BSP and MNOs. While the BSP allowed the market to develop without regulation at first they formalized regulatory requirements to provide legal certainty once the market has reached a critical point.

Figure 12: Key Provisions of the Philippine Central Bank E-Money Circular

### Key Provisions of the Philippine Central Bank E-Money Circular:

- E-Money is defined as monetary value represented by a claim on an issuer that is stored in an instrument or device.
- The device can be cash cards, e-wallets accessible via mobile phones or similar products.
- E-Money can be issued by banks, non-bank financial institutions and non-banks (the latter must apply for “quasi-banking” licenses)
- Issuers must have in place:
  - Sound and prudent management, administrative and accounting procedures
  - Adequate internal control mechanisms
  - Appropriate security policies and measures intended to safeguard the integrity, authenticity and confidentiality of data and operating processes.
  - Adequate business continuity and recovery plan
  - Effective audit function
  - Have at least 100million PHP in paid in share capital
- Places responsibility on issuers to perform KYC, maintain records and monitor e-money movements to conform to AML rules.
- Requires issuers to provide a customer dispute resolution process.
- Puts responsibility on issuers to ensure compliance by their agents with applicable rules and regulations.
- Defines liquid assets requirements and that separate bank deposits must be maintained for liquidity purposes.

### 5.2.5. Relevance to USAID and Implementing Partners

As systemic risk for each of the payment types varies, USAID Missions or Implementing Partners are presented with tradeoffs. For example, cash may be the payment type with the lowest systemic risk, but may be completely unsuitable with respect to financial or other risk types.

## Risk Analysis and Mitigation: *Legal Risk*

For programmatic efforts where a large population of Payment Beneficiaries is receiving funds, the impact of a failure due to systemic risk is made much larger. As payment types are examined for possible risk, it is important to bear in mind the relatively high profile of USAID funds flowing through the system. For example, in the case of disbursing humanitarian aid, not only would a failure constitute undue hardship for Payment Beneficiaries, USAID Missions or Implementing Partners may incur a large amount of reputational risk and cause the payment type to be seen as a total failure. This may serve to stunt the otherwise organic growth of an emerging payment type.

In addition to larger systemic risk evaluation, it is recommended that the parties responsible for the payment be examined using the base guidelines from USAID ADS Chapter 630 as a reference point. Specifically, pre-paid card and mobile payment providers should maintain a viable financial system, compliance with local laws, and the willingness to submit to an audit by a relevant local entity. A good example of adoption of desirable policies in USAID Mission countries comes from The Philippines Central Bank which, in their Circulars No. 649<sup>44</sup> and 704<sup>45</sup> establishes guidelines for safeguards and controls to mitigate risks associated with electronic payment systems and electronic banking – essentially extending appropriate financial system standards and policies to electronic and mobile payments providers.

### 5.3. Legal Risk

Legal risk is defined as a risk which could result in unforeseeable lawsuits, judgment or contracts that could disrupt or affect business practices. The most significant legal risk associated with payments to Payment Beneficiaries is related to compliance with anti-money laundering and terrorism financing regulations. Under AML/CFT legislation, the U.S. government's policy objectives are to ensure that stakeholders in the payment process – and specifically the Mission or Implementing Partner who has liability for successful distribution of funds to Payment Beneficiaries – are able to effectively identify, verify and monitor the distribution of funds in a manner that minimizes the risk that it can be leveraged for money laundering and terrorism financing.

#### 5.3.1. Cash Payments

Cash payments are generally subject to higher legal risk than other payment types. Cash provides neither recipient identification (establishing the identity of the recipient) nor recipient authentication (establishing that the recipient is entitled to receive the funds). Compliance with AML/CFT regulations is a significant legal challenge due to the absence of such verification.

The process for executing cash payments, as described earlier in this report, has been

---

<sup>44</sup> Circular No. 649. Banko Sentral ng Philipinas. <http://www.cgap.org/gm/document-1.9.44821/Circular%20649.pdf>

<sup>45</sup> Circular No. 704. Banko Sentral ng Philipinas. <http://www.bsp.gov.ph/downloads/regulations/attachments/2010/c704.pdf>

## Risk Analysis and Mitigation: *Legal Risk*

established to minimize the risk of misallocation of funds by introducing robust process management and documentation. However, the points of weakness are much more numerous than with other payment types, and documentation is manual and subject to human intervention and error throughout.

### Legal Risk Mitigation – Cash Payments

The financial risk mitigations for cash are also the best method for mitigating legal risk. Additionally, some Implementing Partners will leverage cash transfer agencies or MFIs to disburse funds to un-banked Payment Beneficiaries in order to avoid disbursing physical currency themselves, and to add an additional layer of personal identification and payment documentation. Oxfam has developed well-documented procedures for executing payments through a CTA intermediary, which does provide some legal and financial risk mitigation.

Figure 13: Oxfam Procedures for Cash Payments with a Cash Transfer Agency

Cash Delivery Activity	Actor Responsible
Beneficiary identification	Local partners or Oxfam staff
Beneficiary verification	Oxfam staff
Beneficiary lists prepared including name, ID number, telephone number, address	Oxfam staff
Payment request made to Finance and list sent to Finance	Oxfam staff
List sent to the cash transfer agency (CTA)	Oxfam finance team
CTA sent unique pin numbers per beneficiary that Oxfam then printed on to vouchers	CTA to Oxfam finance team
Vouchers distributed to beneficiaries via partner organizations	Oxfam and local partners
Beneficiaries required to go to the CTA with their vouchers and ID cards in order to receive payment. CTA also sent text message alerts to notify beneficiaries that payments were ready for pick-up.	
Beneficiaries without ID cards had their vouchers stamped with an Oxfam stamp to certify to the bank that Oxfam agreed to the payment	Oxfam staff
Monitoring and evaluation follow-up checks performed on a sub-set of beneficiaries to validate proper receipt	Oxfam staff

It should additionally be noted that transitioning to a payment methodology that allows for stronger mitigation against legal risk is a possible mitigation strategy for cash payments.

### 5.3.2. Electronic Funds Transfer

Legal risk, as defined here, has very similar implications as financial risk, in practice. The risk profiles for EFT and cash are roughly the same as in the case of fraud. There is assumed to be less legal risk with EFT as the sender and recipient have been subject to an identity verification process. Payment Beneficiaries of foreign assistance monies are typically pre-qualified to ensure eligibility, and if they are able to get a bank account or validate their identity for a wire transfer, this creates a relatively low risk scenario with regard to the

## Risk Analysis and Mitigation: *Legal Risk*

misappropriation of funds. The chain of ownership and receipt is all objectively verifiable through bank records.

### Legal Risk Mitigation – Electronic Funds Transfer

In addition to the mitigation strategies described for financial risk, government regulation is an important mitigant against legal risk. In the U.S. FATF regulations require financial institutions to assist the government in detecting and preventing money laundering. There is a specific requirement to report withdrawals or deposits of more than \$10,000 in cash – an amount which may vary based on the country’s economic environment. Financial institutions are also required to monitor and report any suspicious activity.

#### **5.3.3. Pre-paid Cards**

Pre-paid cards, while more digital in nature, can retain some anonymity if not authenticated, and can represent moderate to significant legal risk. In developed countries, pre-paid cards have become prime vehicles for money laundering due to their relatively anonymous nature. Also, pre-paid cards are very portable and allow money to move across country borders with little control. However, in the case of USAID Missions or Implementing Partners it is possible to implement controls to eliminate anonymity and to embed merchant category controls to reduce misuse of funds. This may include Payment Beneficiary pre-screening and post-disbursement verification, as well as pre-paid card distribution controls.

#### **5.3.4. Mobile Payments**

Mobile payments platforms have the potential to reduce financial exclusion and transition the cash economy to a more transparent and traceable digital payment economy. FATF, an inter-governmental body that sets standards to combat money laundering and terrorist financing, has noted that the prevalence of a large, informal, unregulated, and undocumented economy negatively affects AML/CFT efforts and can generate significant money laundering and terrorist financing risks.<sup>46</sup>

There are some unique legal risks associated with mobile transactions due the nature of the mobile payment ecosystem. Namely, the anonymity of the device and the rapidity with which transactions can be conducted present opportunity for money laundering activity.<sup>47</sup> The GSMA has further defined the risk by stage in the mobile money process. Figure 14 details the Mobile Money Methodology for Assessing Money Laundering and Terrorist

---

<sup>46</sup> FATF Guidance Anti-money laundering and terrorist financing measures and Financial Inclusion, June 2011)

<sup>47</sup> While a few countries have passed mandatory identification for cell phone buyers, a bill introduced in the U.S. Congress in the aftermath of the attempted bombing of Times Square in 2010, S 3427 Pre-paid Mobile Device Identification Act, was not passed

## Risk Analysis and Mitigation: *Legal Risk*

Financing Risk.<sup>48</sup>

Figure 14: Mobile Money Methodology for Assessing Money Laundering and Terrorist Financing Risk

General Risk Factors	Loading	Transferring	Withdrawing
<b>Anonymity</b>	Multiple accounts can be opened by criminals to hide the true value of deposits	Suspicious names cannot be flagged by system, making it a safe zone for known criminals and terrorists	Allows for cashing-out of illicit or terrorist funds
<b>Elusiveness</b>	Criminals can “smurf” <sup>49</sup> proceeds from criminal activity into multiple accounts	Criminals can perform multiple transactions to confuse the money trail and origin of funds	“Smurfed” funds from multiple accounts can be withdrawn at the same time
<b>Rapidity</b>	Illegal monies can be quickly deposited and transferred out to another account	Transactions occur in real time leaving little time to stop it if suspicious of terrorist financing or laundering	Criminal money can be moved through the system rapidly and withdrawn from another account

### Pre-paid Cards and Mobile Payments

As with systemic risk, the mitigation strategy for legal risk with regard to electronic payments and mobile payments are quite similar. As leaders in AML/CFT have advocated, legal risk must be considered and regulated in proportion to the magnitude of risk. Without said proportionality, payment systems could become excessively difficult in a given country.

With large percentages of the world’s population currently unbanked, there is a potential for mobile financial services to increase financial inclusion. Imposing strict regulatory burdens that this segment of the population can’t fulfill will keep them excluded from financial access. It will also keep cash payments out of the scope of supervision, thereby enabling the very money laundering and terrorist financing that regulation was enacted to prevent. Current research on this topic advocates that measures be put in place to allow more consumers to use formal financial services to reach the AML/CFT goals.<sup>50</sup>

However, steps must still be taken to minimize legal risk to the extent possible while maintaining focus on financial inclusion. FATF proposes a risk-based approach (illustrated in Figure 15) to decision- and policy-making with regard to AML/CFT objectives. The intent is to retain a firm stance on the criminality of money laundering and terrorism financing, while allowing for sufficient flexibility in the adoption of local policies and standards that

<sup>48</sup> Adapted from “GSMA Mobile Money for the Under-Banked: Mobile Money Methodology for Assessing Money Laundering and Terrorist Financing Risk”, page 15

<sup>49</sup> Smurfing is the practice of executing financial transactions (such as the making of bank deposits) in a specific pattern calculated to avoid the creation of certain records and reports required by law

<sup>50</sup> 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. World Bank, Washington, DC

## Risk Analysis and Mitigation: *Legal Risk*

balance benefits (financial inclusion) with legal risks.<sup>51</sup>

This approach allows governments and private institutions, depending on which is driving modernization in the area of electronic and mobile payments, to focus on due diligence and prevention within the framework of an accepted benefit/cost determination. By adopting such an approach, competent authorities and financial institutions are able to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified.

The GSMA has also developed a Methodology for Assessing Money Laundering and Terrorist Financing Risk, which is illustrated in Figure 15, below. The Methodology elaborates a systematic approach for assessing the vulnerabilities of mobile money to legal risks, understanding how these vulnerabilities could be exploited by money launderers and terrorists, and identifying appropriate and effective tools to mitigate identified risks.<sup>52</sup>

**Figure 15: Comparative risks of mobile money and cash, before and after controls applied**

General Risk Factors	Mobile Money Before Controls	Mobile Money After Controls	Description of Controls
Anonymity	High Risk	Low Risk	<ul style="list-style-type: none"> <li>Customer profile building – includes registration info (name, unique phone number, etc.)</li> </ul>
Elusiveness	High Risk	Low Risk	<ul style="list-style-type: none"> <li>Limits on amount, balance, frequency and number of transactions</li> <li>Real-time monitoring</li> </ul>
Rapidity	Low Risk	Low Risk	<ul style="list-style-type: none"> <li>Real-time monitoring</li> <li>Frequency restrictions on transactions</li> <li>Restrictions on transaction amount and total account turnover in a given period</li> </ul>
Lack of Oversight	High Risk	Low Risk	<ul style="list-style-type: none"> <li>N/A</li> </ul>

A variety of risk-mitigation processes are also discussed, including implementing measures that reduce the risk of money laundering and terrorism financing by consumers. For example, GSMA recommends establishing limits on accounts and transactions, monitoring transaction frequency and implementing automated tracking of transaction flows on the system level. These recommendations have already been implemented by active mobile payment providers. M-Pesa in Kenya, for instance, places limits on the amount of funds that can be transacted (maximum of 70,000 Ksh leaving the account daily – about \$818) and stored (maximum account balance is 50,000 Ksh, or about \$584).<sup>53</sup> Similarly, Tcho Tcho Mobile in Haiti sets a maximum account balance of 4,000 HTG (\$100) or 10,000 HTG (\$250), depending on the type of account. Daily transactions are similarly limited.<sup>54</sup>

<sup>51</sup> FATF: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, February 12th

<sup>52</sup> GSMA Mobile Money for the Under-Banked: Mobile Money Methodology for Assessing Money laundering and Terrorist Financing Risk, page 18.

<sup>53</sup> 10 Things You Thought You Knew About M-Pesa. CGAP. November 22, 2010.

<http://technology.cgap.org/2010/11/22/10-things-you-thought-you-knew-about-m-pesa/>

<sup>54</sup> Haiti Leads in Mobile Payments. Partners in Pre-paid. April 23, 2012.

<https://www.partnersinpre-paid.com/topics/articles/haiti-leads-in-mobile-payments.html>

## Risk Analysis and Mitigation: *Operational Risk - General*

By assessing risk both before and after such mitigating controls are in place, service providers and regulators can evaluate the appropriateness of such mechanisms. A risk assessment once such controls have been applied then becomes an input to the establishment of standardized customer due diligence requirements that are appropriate to the unique risk profile of a given environment.

### **5.3.5. Relevance to USAID and Implementing Partners**

USAID is in a position to encourage Missions and Implementing Partners to evaluate electronic and mobile payments providers based on the standards and practices they have put in place with regard to AML/CFT, as well as the degree to which they have identified and documented the unique risk profile of the local environment. Missions working with local governments have been able to assist in this way with the development of local regulation. Ideally, payment providers will have also established reasonable and logical customer due diligence procedures that will help to mitigate legal risks. The concept of customer due diligence is addressed again in the section on operational risk as customer identification and authentication also have a broad operational, fraud and legal impact.

## 5.4. Operational Risk - General

Operational risk is defined as a risk which damages the ability of one of the stakeholders to effectively operate their business, or results in a direct or indirect loss from failed internal processes, people, systems or external events. More generally, and for the purpose of evaluating both current payment types and electronic and mobile payments, operational risk can be defined by the extent to which funds are accessible and security of funds for the execution of payments.

A number of sub-risks can be categorized as operational risks. This analysis examines:

- Interoperability
- Customer identification and authentication
- Provider governance

Operational risks are significantly different for mature payment types (EFT and cash) than they are for pre-paid cards and mobile payments. For ease of understanding, this section focuses on general accessibility and security-related operational risks for EFT and cash payments only. The following sections will go into each of the three operational sub-risks in the context of electronic and mobile payments.

### **5.4.1. Cash Payments**

Cash transactions require that currency be physically distributed by the Implementing Partner or one of their agents. This process undoubtedly creates both logistical and security challenges. For example, customer identification verification can be difficult in

## Risk Analysis and Mitigation: *Operational Risk - General*

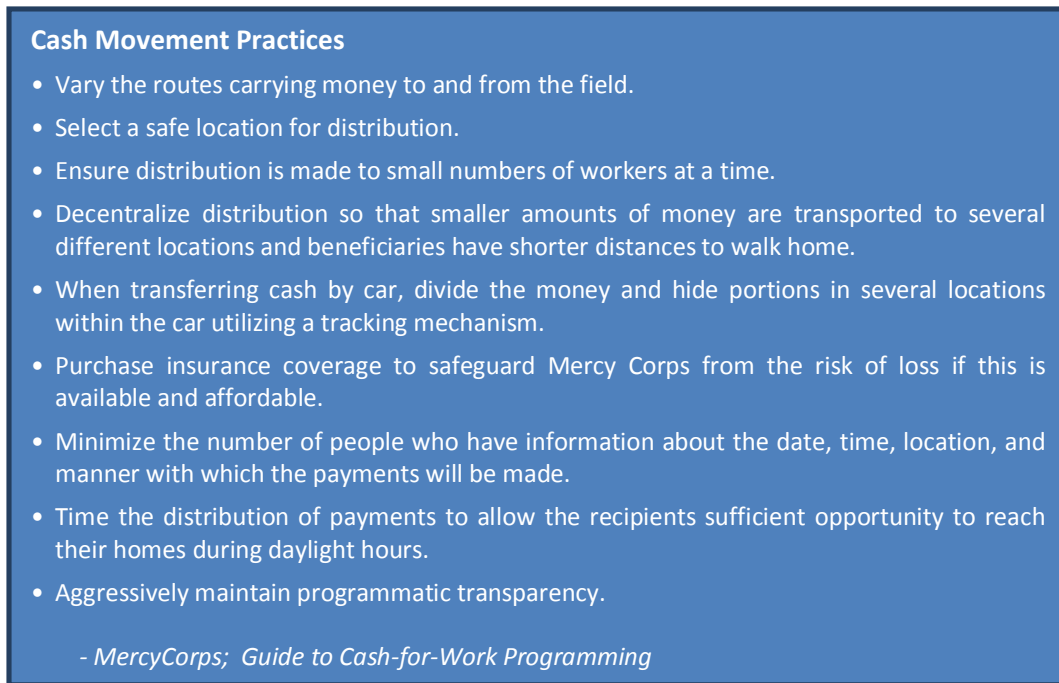
regions with no national identification system. This can lead to identification issues that can result in fraud and the misappropriation of funds. In addition, there is significant opportunity for theft throughout the transfer process, and once stolen or redirected, cash can be easily reused without any traceability. Operational risk with cash is significant.

### Operational Risk Mitigation – Cash Payments

The most important aspect of operational risk for cash is physical security of currency. Standards and practices for the safe storage and transportation of cash can be implemented to mitigate this form of operational risk.

Many USAID Implementing Partners have developed best practices for cash payments, based on their experience in the field, that help to mitigate accessibility and security risks.

Figure 16: Cash Movement Practices



**Cash Movement Practices**

- Vary the routes carrying money to and from the field.
- Select a safe location for distribution.
- Ensure distribution is made to small numbers of workers at a time.
- Decentralize distribution so that smaller amounts of money are transported to several different locations and beneficiaries have shorter distances to walk home.
- When transferring cash by car, divide the money and hide portions in several locations within the car utilizing a tracking mechanism.
- Purchase insurance coverage to safeguard Mercy Corps from the risk of loss if this is available and affordable.
- Minimize the number of people who have information about the date, time, location, and manner with which the payments will be made.
- Time the distribution of payments to allow the recipients sufficient opportunity to reach their homes during daylight hours.
- Aggressively maintain programmatic transparency.

- MercyCorps; *Guide to Cash-for-Work Programming*

### **5.4.2. Electronic Funds Transfer**

It is clear, based on the analysis of current payment types, that there is significantly higher operational risk associated with cash than with EFT. EFT payments presuppose that both the distributor of funds and the Payment Beneficiary have bank accounts. In this case, funds accessibility and security are guaranteed by the bank. In a given USAID Mission environment, operational risk related to EFT is negatively correlated with the strength and maturity of the banking sector.

### Operational Risk Mitigation – Electronic Funds Transfer



Mitigations for operational risk in EFT payments are related to proper assessment of banking sector strength and stability, as well as a review of bank policies with regard to guarantee of payments, transfers and insurance of funds.

### **5.4.3. Relevance to USAID and Implementing Partners**

Operational risks are perhaps the most significant consideration for USAID, as this risk category serves to highlight important differences in the way the four payment types function in practice. As will be made clear in the following sections, a number of new operational risks must be considered with the introduction of electronic and mobile payments, and, if evaluated in a vacuum, those risks may result in a biased evaluation. When applying this information to a country-specific payments evaluation, Mission personnel and Implementing Partners should consider risks related to interoperability, electronic customer authentication and provider governance in parallel to realistic evaluation of funds security risks for cash and EFT transactions.

## **5.5. Operational Risk - Interoperability**

Interoperability risk is defined as the lack of inter or intra network operability that may prevent a consumer from transacting with the desired party. Interoperability has become one of the major points of contention in recent discussions of electronic and mobile payments.

### **5.5.1. Electronic and Mobile Payments**

In order for electronic and mobile payment systems to be interoperable, three conditions must be met:

1. Transactions and message formats must be standardized. As an example, the VISA and MasterCard networks adhere to ISO 7813 for the formatting of magnetic stripe cards.<sup>55</sup> Merchants know that card readers must accept this message format, and processors and banks accept messages in this format.
2. Exchange of information between platforms enabled via a switch. As an example, the VISA and MasterCard payment networks operate switches that connect to the acquirers (merchant processors) and to the issuers (banks).
3. Commercial agreement between payment system participants. In the case of the credit card industry, clear requirements have been defined for merchants and banks to become participants. Once they participate in the system, the network sets a pricing structure that negates the need for individual merchant – bank negotiation.

---

<sup>55</sup> International Standards Organization, <http://www.iso.org/iso/home.htm>

## Risk Analysis and Mitigation: *Operational Risk - Interoperability*

A certain level of interoperability has been achieved for electronic payments in the form of pre-paid cards. As long as a merchant has a point-of-sale device that can accept card transactions for the associated payment network, the underlying technology is in place to transfer payment data regardless of the data service provider.

True interoperability has not yet been achieved for mobile payments. Market competition in mobile network technology has resulted in the development of different transaction sets and message formats. There does not yet exist a mobile operator “switch” that could be compared to the switches operated by payment networks.

Beyond just technology issues, there are interoperability issues related to business relationships. The multiple players in the mobile payments ecosystem have yet to establish general economic terms of participation, indicating roles, fee structures for network transfers and terms for data-sharing.

### *Operational Risk (Interoperability) Mitigation*

Governments and non-governmental industry standards bodies have adopted a number of approaches in an attempt to improve standardization and interoperability. The Consultative Group to Assist the Poor (CGAP), a consortium of 33 public and private development agencies housed by the World Bank, has defined three levels of interoperability that need to be addressed and are relevant to USAID decision-making.

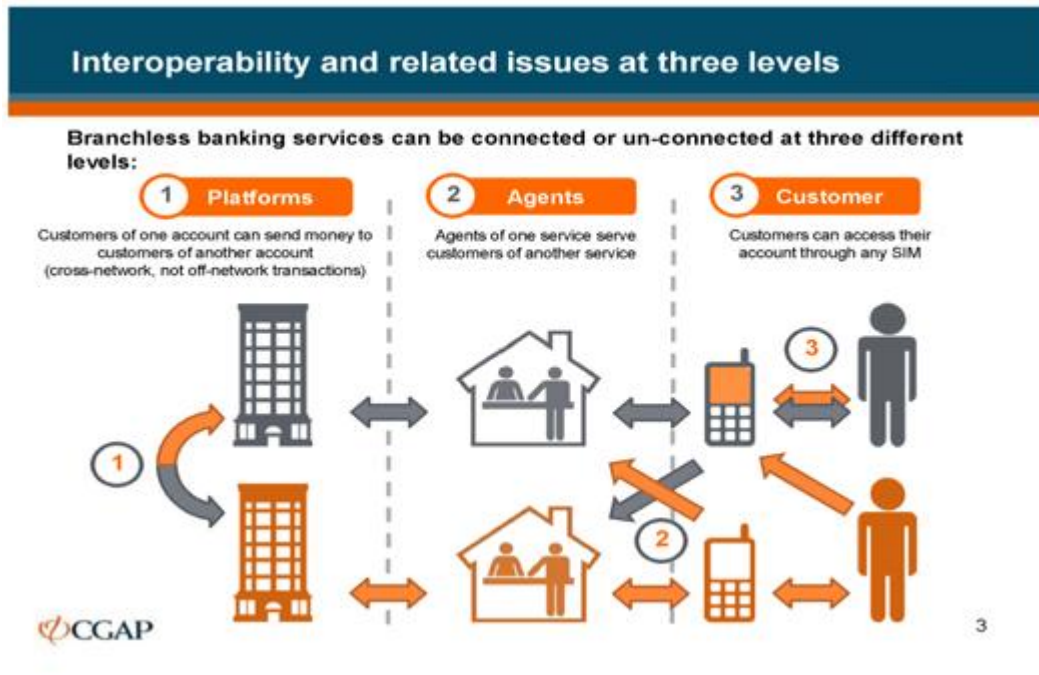
1. **Platform-level interconnection** – If mobile money platforms are interconnected, a customer with an account with one service provider can send or receive money to or from the account of a customer with a different service provider. To date platform-level interconnection has not been implemented widely.
2. **Agent-level exclusivity** – Agent exclusivity revolves around the ability of a customer of one provider to use the agent of another provider for cash-in/cash-out services related to that customer’s account. Agent interoperability is possible even when there is agent exclusivity, as long as platforms are interconnected (such as with interoperable ATM networks).
3. **Customer-level interoperability** – This term is used to describe two interoperability scenarios related to the mobile handset:
  - a customer’s ability to access his/her account using any phone with a SIM card on the same network
  - a customer’s ability to access multiple accounts on one SIM<sup>56</sup>

Figure 17 illustrates these interoperability levels in more detail.

---

<sup>56</sup> Interoperability and related issues in branchless banking and mobile money: by Kabir Kumar and Michael Tarazi : Monday, January 9, 2012

Figure 17: Interoperability Issues<sup>57</sup>



The question of interoperability needs to be addressed on a systemic level, as emerging mobile money providers typically have little incentive to ensure interoperability, favoring competition and the opportunity to increase revenues through exclusivity. At the same time it is in the interest of the mobile eco-system as a whole to accelerate the level of participation in mobile money programs. The incentive for individual consumers to participate increases as the number of other users and acceptance points increases.

For these reasons, establishing and enforcing common standards to ensure interoperability is currently in the domain of national governments or supra governmental organizations. The extent to which this occurs, and the effectiveness of such efforts will, of course, vary from country to country, however there are some international standards that can be used to develop local policies. The European Union, for example, has released Mobile Contactless Single Euro Payments Area (SEPA) Card Payments Interoperability Implementation Guidelines (EPC<sup>58</sup> 178-10) through its European Payments Council. The stated objectives for these guidelines include:

- Enable the quick development and implementation of mobile solutions.
- Avoid the development of proprietary solutions with limited (geographical) reach, leading to fragmentation of the market.
- Provide transparency to market participants for the Mobile Contactless SEPA Card payments by describing the roles of the large number of stakeholders involved.

<sup>57</sup> Interoperability and Related Issues in Branchless Banking: A Framework, CGAP

<sup>58</sup> EPC stands for European Payments Council

## Risk Analysis and Mitigation: *Operational Risk - Interoperability*

- Clarify the position of the European Payments Council (EPC) to ensure the interests with regard to standardization and industry bodies.
- Define the minimum level of security for the whole mobile payment value chain in order to establish confidence in this environment.<sup>59</sup>

In contrast to the concerted effort made by the European Union, there are few individual countries that have developed interoperability mandates. In many markets, however, industry associations and standards bodies have started formulating interoperability standards that local country competitors can adopt to support growth in their local markets. One example is the Mobile Payments Forum of India (MPFI) and the Interoperability Standards for Mobile Payments. The standards cover typical transaction flows as well as technical and security standards.

In many markets, MNOs are leading the development of mobile payment system standards. The GSMA, a global MNO trade organization, weighs the consumer demand for interoperability and the investment required on the part of mobile money stakeholders.

*Given that the “walls” in the walled gardens of mobile money are, as we have seen, porous, it is not obvious that imposing interconnection would create significant welfare gains for customers. Indeed, it might have the opposite effect, if mobile operators must raise prices or curtail investment in other areas in order to implement interconnectivity.<sup>60</sup>*

While global standards and leading practices are still emerging, there are some examples in the market of successes in interoperability for mobile payments. For example, M-Pesa allows consumers to send money to any phone, even outside of the Safaricom network (which is M-Pesa’s exclusive partner). Non-Safaricom Payment Beneficiaries are sent a voucher with a one-time PIN, which they can take to Safaricom agents to withdraw cash. This is not a technology solution to interoperability, but it does allow for mobile payment execution across networks.

There are similar examples for pre-paid cards. Smart Communications in the Philippines has partnered with MasterCard to issue Smart Money MasterCard debit cards that enable consumers to use their mobile money wherever MasterCard is accepted, domestically and internationally. Wizzit in South Africa has done the same thing. Where ATMs are available, Wizzit subscribers can use their Wizzit MasterCards to deposit and withdraw cash. Where merchants have MasterCard terminals at the POS, Wizzit subscribers can use their cards to make payments using their Wizzit accounts.<sup>61</sup>

---

<sup>59</sup> Mobile Contactless SEPA Card Payments Interoperability Implementation Guidelines

<sup>60</sup> GSMA — Mobile Money for the Unbanked. The case for interoperability: Assessing the value that the interconnection of mobile money services would create for customers and operators

<sup>61</sup> Developing Mobile Ecosystems, Beth Jenkins

## Risk Analysis and Mitigation: *Operational Risk - Customer Identification and Authentication*

### 5.5.2. Relevance to USAID and Implementing Partners

With respect to USAID Missions or Implementing Partners investigating the use of mobile payments, interoperability may be one of the most important factors. The idea of mandating use of a specific MNO in order to receive funding is counter to effective delivery of foreign aid. As noted in prior sections, when examining payment types that differ from the current state, a thorough analysis of benefits to Payment Beneficiaries is strongly recommended. However, in the interim USAID may find it beneficial to collaborate with either direct or indirect stakeholders to support mitigation of interoperability risk. This may include:

- **Standards Development** – Similar to the standards that have been set by the mobile industry to facilitate the sending and receiving of SMS messages, standards for mobile payments could be developed by payment networks or mobile operator associations such as GSMA or Cellular Telecommunications and Internet Association (CTIA). This approach might be premature as the market is still developing new technical solutions and innovation could be dampened. However, it is possible USAID could be a key collaborator in this process.
- **Payment Hubs** – Create payment hubs that participants in the market can connect to similar to payment switches. This is an approach that will require an upfront commitment by a group of market participants in the software and hardware industries. Potentially, this investment could include participation from USAID.
- **Coalition Building** – In the absence of standards or hubs, bi-lateral agreements between service providers can expand access for the user base of both service providers without having to gain cooperation of all participants in the marketplace.

Given the current state of development with regards to interoperability, it is unrealistic to expect all mobile money providers to become interoperable in the near term. In the meantime, this might mean engaging with more than one mobile payment provider in a given country to ensure the largest possible number of participants. Also, if mobile payment providers can offer more than at least one channel for cash out that goes beyond their own networks that might be a first step towards encouraging more interconnection and interoperability.

### 5.6. Operational Risk - Customer Identification and Authentication

The risks identified in this category center on the ability to identify that the party executing a transaction is in fact valid. For the purposes of mitigating the risk of money laundering, terrorist financing, ghost recipients, and other funds misuse, this risk category requires careful consideration.

In order to validate a customer, identity must be addressed at both account set-up (identification) as well as account usage (authentication), and measures must be taken to ensure that customer identity and data are maintained in a secure way. Several

## Risk Analysis and Mitigation: *Operational Risk - Customer Identification and Authentication*

approaches have been identified by USAID, international standards bodies and in-country regulation to address these questions.

In this section we look in detail at the requirements for conducting customer due diligence, best practices in customer authentication and finally data security standards for personally identifiable customer data.

### **5.6.1. Electronic and Mobile Payments**

Operational risk related to customer identification and authentication for electronic and mobile payments is very similar to financial and legal risk. If a payment system is unable to reliably and consistently validate the actors in a payment transaction, the risk of fraud and misallocation of funds for illicit purposes is present. Customer identification and transaction monitoring not only help to mitigate against money laundering, but also play an important role in marketing and fraud prevention.

#### *Operational Risk (Customer Identification and Authentication) Mitigation*

##### *Customer Identification*

The process to address the initial customer identification must be designed to address the following areas:

- Customer Data Requirements – What do we need to know about the customer?
- Sources of Identification – What documentation exists to validate that information?
- Identifying Entity – Who is authorized and required to collect the information from the customer?
- Place of Identification – How and where is identification performed?

While global standards for this process continue to emerge, FATF has provided guidelines with respect to the due diligence process for financial institutions. Specifically, “[u]nder AML/CFT legislation, customer due diligence (CDD) policy objectives are to ensure that financial institutions can effectively identify, verify and monitor their customers and the financial transactions in which they engage, in accordance to the risks of money laundering and terrorism financing that they pose.”<sup>62</sup> These guidelines, in addition to approaches identified by USAID, in-country regulators, and other international standards bodies, provides a framework for addressing each of the four aforementioned areas.

Figure 18 provides a table for assessing the different types of customer identification processes and actors typically available in countries where electronic and mobile payments are an option.

---

<sup>62</sup> FATF Guidance, Anti-money laundering and terrorist financing measures and Financial Inclusion, page 25

## Risk Analysis and Mitigation: *Operational* Risk - Customer Identification and Authentication

Figure 18: Assessment of Customer Identification Processes

	Weak	Good	Superior
<b>Customer data requirements</b>	Name Address Date of Birth	Name Address Date of Birth Phone Number SIM Card	Name Address Date of Birth Identification Number Phone Number SIM or pre-paid card ID
<b>Documentation sources</b>	Other ID	Third party database Financial ID	National ID Biometrics
<b>Identifying entity</b>	Agents	Bank MNO Licensed Agent	Government Entity
<b>Place of identification</b>	Non face to face	Electronic	Face to face

A major component of these guidelines is related to customer data requirements. Regulators have provided frameworks for banks and other financial institutions to develop Know Your Customer (KYC) rules. The requirements should be tiered according to the nature of the relationship and transaction sizes typically conducted in these account. Providers of credit, debit and pre-paid cards have adopted variations of KYC rules and it is reasonable to assume they provide a good baseline for information that should be collected for new mobile money customers in equivalent environments.

Additionally, the Customer Identification Program (CIP) final rule, interpreting Section 326 of the USA Patriot Act<sup>63</sup> provides the following minimally required data elements for opening individual customer accounts.

- Name
- Date of Birth
- Residential address
- Identification number

In addition to these data elements, mobile money initiatives have access to the unique identifiers of Phone number and SIM card ID, and pre-paid card transactions have the ability to track payments through the unique payment card ID number.

The core of any customer identification effort is dependent on the available documentation.

*Policy makers should consider measures to strengthen and standardize the national identification systems. This single policy initiative will not only improve all financial Account Providers' ability to perform CDD/KYC as an effective tool for financial inclusion but, concomitantly, serves as a*

<sup>63</sup> USA Patriot Act of 2001. Public Law 107-56—Oct. 26, 2001, Section 326.

## Risk Analysis and Mitigation: *Operational Risk - Customer Identification and Authentication*

*cornerstone of AML and CFT compliance measures. In lieu of national IDs, alternative instruments, such as financial IDs, should be considered and enumerated by appropriate State authorities.<sup>64</sup>*

Realistically, there are countries in which USAID Missions and Implementing Partners operate where no government issued ID exists, where birth records are unavailable and where residential addresses are not used. If possible identity should be verified through alternative sources. For example, if available, third party databases or financial IDs established by banking consortia or credit agencies can provide an alternative source. However, making use of such resources requires thorough and well-structured due diligence on the part of the payment provider. The proper standard of due diligence, however, is not static and should be commensurate with the risk profile of the payment environment.

Compliance of customer due diligence processes with any established national standards is dependent upon the entity performing the due diligence. In some countries the identification of potential customers is performed by government agencies, which is generally considered to be the strongest form of customer identification. As a standard business practice, customer identification should be performed by the account holding entity, whether that is a bank, credit card company or MNO. As discussed below in the section on agent governance, the process for performing customer due diligence can also be performed by a third party, but the responsibility remains with the account holding entity.

Regarding place of identification; ideally identification happens face to face where a representative of the account holding entity can verify the identity of the account holder. If a non-face to face process is used, other aspects of the customer identification process should be strengthened.

### *Customer Authentication*

Once a customer's identity has been confirmed and an account set up, the customer has to be provided with tools to access his or her account that will identify him as the authorized user. For card-based electronic payments there are two types of points of interaction (POI) where consumers are authenticated: POS payments and Card Not Present (CNP) transactions, such as on-line shopping.

The strengths and limitations of current card based customer authentication methods are apparent. At the POS, customers are authenticated by presenting their card and signing the receipt where the signature is compared to that on the card, or by entering a PIN that is validated off-line or on-line.

---

<sup>64</sup> USAID Mobile Financial Services Risk Matrix , published by USAID in July 2011



## Risk Analysis and Mitigation: *Operational Risk* - Customer Identification and Authentication

In CNP transactions, customers enter their card details but there is currently no widely accepted method for validating that the transaction is being conducted by the authorized user. (VISA and MasterCard have launched additional verification tools such as MasterCard Secure Code but they have not been adopted widely). Fraud in CNP transactions therefore tends to be more common than fraud at the POS. One method increasingly used by on-line merchants and banks is to perform “device fingerprinting” that prevents IP addresses originating from high risk areas from transacting.

Building on best practices from card-based electronic payments and leveraging the additional data provided by the mobile device, the best practice for mobile financial services authentication is two-factor authentication. Two-factor authentication is best described as something that you have (phone, SIM card) and something that you know (a bank issued PIN). This helps to address efforts to defraud a mobile payment system through “spoofing” of SIM IDs in a single authentication transaction. This occurs when an attacker sends SMS messages into the messaging network with “spoofed” originator IDs in an attempt to either withdraw money from the account, or to encourage the mobile account-holder to send funds to a fraudulent recipient.<sup>65</sup>

The leading mobile carrier association in the U.S. CTIA has published best practices and guidelines on customer authentication, including:

- **Encourage regular PIN changes** – Offer the opportunity for customers to change their PINs on a regular basis. This reduces the risk of jeopardizing an old PIN. Note the difference between a SIM/phone PIN and a bank-issued PIN.
- **Provide tiered access** – Base available functionality on the level of authentication used to access the service.
- **Use information available** – Certain unique information about the SIM card (IMSI) may be obtained working in cooperation with the network service providers. Use this information as a second factor authentication mechanism, to allow you to identify when a fraudulent SIM swap happens.<sup>66</sup>

Banks and financial institutions habitually use two-factor authentication technology to provide a secure method for mobile banking. While there are still vulnerabilities, it remains one of the most common security platforms being used for customer authentication in mobile banking solutions.

### *Customer Data Security*

Strong customer authentication processes are essential to verify that card and mobile device transactions are conducted only by authorized users. Unfortunately, breaches at

---

<sup>65</sup> Risks and Threats Analysis and Security Best Practices: Mobile 2-Way Messaging Systems. Mobile Payment Forum. May 13, 2003.

<sup>66</sup> Best Practices and Guidelines for Mobile Financial Services. CTIA

## Risk Analysis and Mitigation: *Operational Risk* . Provider Governance

card processors have increased, and the importance of safeguarding customer data cannot be overemphasized.

Maintaining customer data security is a challenge for which the electronic payments industry has put standards in place, namely the Payment Card Industry (PCI) standard. In major debit and credit card markets, PCI Data Security Standard (PCI DSS) compliance is required for all entities that store, process and/or transmit cardholder data. While compliance with PCI standards<sup>67</sup> is perceived to place a reporting and financial burden on payment system stakeholders, adoption of the standards has helped reduce fraud across the system. CTIA has adapted the card industry's PCI DSS to ensure protection of customer data on the phone:

*For Mobile Phone Banking PCI potentially applies on several levels. Securing the network that stores, processes and/or transmits cardholder data. Ensuring the devices used are PCI [PIN Entry Device] PED or Encrypting PIN Pad (EPP) compliant. Ensuring the devices use only applications that comply with the [Payment Application Data Security Standard] PA-DSS requirements such that cardholder activity is always secured.<sup>68</sup>*

### 5.6.2. Relevance to USAID and Implementing Partners

Mitigating customer identification and authentication risk is critical to the proper design of any program that includes payments to Payment Beneficiaries. In the case of cash payments, USAID Missions and Implementing Partners have long been addressing this concern through the use of potentially cumbersome processes and burdensome logistics. (See Figure 5 in Section 3.2.2.) USAID understands that when examining new payment types, it is important that lower cost processes or logistics not undermine the need for identification and authentication.

The importance of examining customer identification and authentication risk is increased as the funds flowing through potential payment types originate within a U.S. government agency. Without a fully documented, reasonable, and acceptable process in place, an issue with customer identification and authentication could rapidly translate into reputational risk as well as systemic risk for either USAID or a payments environment.

## 5.7. Operational Risk – Provider Governance

Operational risks related to provider governance are those in which the risks to customer funds arise out of a lack of appropriate governance structure, standards and practices within the provider organization. An example might be the inability to access funds due to systems outages or instability of credit due to improper screening of account holders.

---

<sup>67</sup> See Appendix A.4. for PCI DSS Rules

<sup>68</sup> Best Practices and Guidelines for Mobile Financial Services. CTIA

## Risk Analysis and Mitigation: *Operational Risk* . Provider Governance

Provider governance is of key importance as it is in an organization's internal processes and controls that regulation and international best practices get implemented. As has been discussed in previous risk sections, implementation of such controls and best practices are often the best risk mitigation strategy.

### 5.7.1. Electronic and Mobile Payments

Poor provider governance can result in a number of risks to the consumer and the systems. The most important of these are:

- Lack of provider stability and the potential loss of a customer's funds.
- Lack of sufficient agent supervision and the potential for fraud.

Whether the account holder is a MNO or a bank, the provider of the mobile money service will play a key role in ensuring the execution of the end-to-end financial transaction.

#### *Operational Risk (Provider Governance) Mitigation*

Ensuring that the provider selected to operate a pre-paid card or mobile money service has the adequate processes and controls in place is the first step to minimizing risks arising from poor provider governance. While there are specific requirements that the local partner needs to meet in order to address these potential risks, the first screening process should use the general intent of the USAID ADS 630.

Mobile money providers need to demonstrate that they are able to deliver the service to the intended recipient in a compliant way. This includes having robust standards and procedures for governance and operations and infrastructure that adhere to best practices commonly associate with financial institutions and/or those advocated by organizations like the GSMA.

Mobile money providers should also demonstrate awareness of regulatory guidelines that apply to mobile payment products and services, produce a plan to ensure compliance with such regulation, provide reporting on operational metrics and be able to flag potential compliance issues.

Figure 19 below details the areas in which standards and procedures should be evaluated when considering the state of provider governance.

## Risk Analysis and Mitigation: *Operational Risk* . Provider Governance

Figure 19: Provider Governance Standards and Procedures Summary

Governance	Operations and Infrastructure
<ol style="list-style-type: none"> <li>Established Standards and procedures for:                             <ul style="list-style-type: none"> <li>Account opening</li> <li>Transaction processing</li> <li>Dispute resolution</li> <li>Refunds</li> <li>Clearing</li> <li>Settlement</li> </ul> </li> <li>Agent management standards and procedures:                             <ul style="list-style-type: none"> <li>Agent selection</li> <li>Contracting</li> <li>Agent processes and procedures</li> <li>Service level standards</li> <li>Training</li> <li>Supervision</li> </ul> </li> <li>Data privacy and security policies</li> </ol>	<ol style="list-style-type: none"> <li>Underwriting department:                             <ul style="list-style-type: none"> <li>Detailed process for capturing and retaining applicant data.</li> <li>Detailed process for obtaining third party information</li> <li>Detailed process for setting up accounts and assigning account numbers</li> </ul> </li> <li>Risk department:                             <ul style="list-style-type: none"> <li>Account opening criteria</li> <li>Risk review policies</li> <li>Fraud monitoring and detection</li> </ul> </li> <li>Customer Service:                             <ul style="list-style-type: none"> <li>Dispute management</li> </ul> </li> <li>IT:                             <ul style="list-style-type: none"> <li>Provide detailed architecture overview</li> <li>System availability</li> <li>Data center physical security</li> </ul> </li> <li>Finance:                             <ul style="list-style-type: none"> <li>Document process used to set up and maintain trust accounts</li> </ul> </li> </ol>

Mobile money providers have also developed and rolled out transaction confirmation processes that provide transaction documentation for control and audit purposes. This documentation is available on-line and includes sender, recipient, amount, date and transaction status. Two examples are included below. Figure 20 shows the “Completed Transaction Report” provided by Orange Money.

Figure 20: Orange Money Completed Transaction Report

Logged in as: 1441 | PNBUC  
 Organisation: TELKOM KENYA LIMITED-ORANGE MONEY  
 Roles: Verifier  
 Log Out

PERSONAL PROFILE TRANSACTIONS REPORTS HOME

Use this page to view uploaded bulk payment transactions

Start Date: 28-Oct-2011 0000 End Date: 23-Oct-2011 2359

Page Size: 20

Status: All

Go Clear

Bulk ID	Bulk Name	Date	Validator	Transfer	Confirmation	Payment Total	Receipt/Invoice Total	Withdrawal Fee	Status	Action
561	STAFFCLASH17102011	2011-Oct-17 15:50	dkh	dpf	gmbuj	63698	00	00	completed	More details

Bulk details for 561 with description "STAFFCLASH17102011"

Receiptment	Account	Name	Amount	Change to Resources	Change to Recipient	Status	Payment Status
254774140			7100	00	00	Completed	Paid
254770251			30000	00	00	Completed	Paid
254772771			1600	00	00	Completed	Paid
254770071			2560	00	00	Completed	Paid
764770090			8148	00	00	Finalized	Not

Figure 21 shows a similar report from M-Pesa.

Figure 21: M-Pesa Completed Transaction Report

Beneficiary Name as uploaded	Bank Code	Account Number	Amount	Transaction Number	M-Pesa Transaction Code	Validated Name & Number
Ve Aw	99-002	XXXXXXXX	6,075.00	977670001	BN68YQ787	0' V
Ch Atl	99-002	XXXXXXXX	4,445.00	977670002	BN68YX887	0' C N
Ed Od	99-002	XXXXXXXX	4,445.00	977670003	BN67UH846	0' E
Ke On	99-002	XXXXXXXX	4,445.00	977670004	BN67UL481	0' K O
Me Ou	99-002	XXXXXXXX	4,445.00	977670005	BN68ZA163	0' N
Ve An	99-002	XXXXXXXX	4,445.00	977670006	BN67UH207	0' V O

### 5.7.2. Relevance to USAID and Implementing Partners

USAID should encourage Implementing Partners to conduct due diligence with respect to provider governance. For example the existence of adequate provider governance reduces risks associated with Payment Beneficiary identity. This may be especially important in post or current conflict environments where the perception of receiving funds from the U.S. government could cause physical security and safety concerns. Additionally, the presence of sufficient internal and governance controls can serve to mitigate risks created by an immature regulatory or enforcement environment.

### 5.8. Technology Risk

Technology risk is defined as the risk that technology failure will result in a direct or indirect loss to a stakeholder in the payment process. All payments methods, with the exception of cash, are operated using technology solutions. For all of these payment methods technology risk exists. The most significant technology risk is associated with electronic and mobile payment methods that are vulnerable to attack through hardware (phone or POS devices), software (web browsers and applications), and communications platforms (wireless or mobile networks). Risks unique to payment methods are discussed in detail below, however a number of higher-level technology risks should be noted. Specifically, payment methods that rely on a technology service platform will experience overarching risks of service outages and technology evolution (and eventual obsolescence). This is, of course, true of any industry, but the significance of this risk should not be overlooked when considering impact on Payment Beneficiaries.

## Risk Analysis and Mitigation: *Technology Risk*

The frequency of service and power outages in local environments that would affect the ability of Payment Beneficiaries to access funds are an important environmental condition, and a contributor to the overall technology risk for EFT, pre-paid cards and mobile payments. This kind of risk it typically difficult to mitigate at the program-level, so it is better considered as a precondition to adopting any electronic payment type.

The risk of technology evolution and eventual obsolescence has fewer short-term implications for Payment Beneficiaries. Evolutions within a payment technology tend to be incremental and backwards compatibility is typically taken into consideration by providers in order to encourage adoption. However, technological capability may also evolve to make a payment technology obsolete. For example, if a new form of technology-specific authentication is developed, it could make older iterations of similar technology without such authentication capability obsolete. This kind of risk should be a consideration when determining suitability for USAID programs.

### **5.8.1. Cash Payments**

Cash payments are executed through physical in person methods. These methods are not supported by technology solutions and do not require technology to operate. As a result, no technology risks exist for cash payment methods.

#### *Technology Risk Mitigation – Cash Payments*

As above, cash risk not applicable.

### **5.8.2. Electronic Funds Transfer**

EFT payments are executed using inter/intra-bank payment system technology. As previously described, these operate on a switch system used by banks to direct payments. For inter-bank payments this switch is generally a secure payments platform that operates with powerful encryption security technology. For intra-bank payments the security of the system is dependent on the maturity and sophistication of the solution in place in each particular institution. The primary technology risk for this payment method is system outage failure. This can be caused by either hardware or software failures or by network power failures.

Additionally, these systems are vulnerable to cyber-crime, whereby the system is targeted by cyber-criminals with the objective of stealing confidential payments information or embezzlement. This is considered a lesser risk due to the insulation of the systems on bank platforms within the banking network and the relative sophistication of system security and procedural controls.

#### *Technology Risk Mitigation – Electronic Funds Transfer*

## Risk Analysis and Mitigation: *Technology Risk*

For EFT payments vulnerable to system outages due to country utility infrastructure issues risks can be mitigated by individual institutions. This can be achieved through the establishment of disaster recovery programs and the maintenance of independent power facilities and offsite system replication capabilities. This type of emergency contingency planning is a standard part of corporate practice in developed economies. USAID can encourage institutions to make contingency planning part of standard business practices to reduce the risk from utility infrastructure issues.

Mitigating cyber-crime activities is achieved through investment in system security and procedural control enhancements. Regarding the cyber-crime vulnerability of intra-bank payments systems, each system and the associated disbursement procedures must individually be evaluated against international standards to reduce exposure to risk from fraud and embezzlement.

### **5.8.3. Pre-paid Cards**

Pre-paid card payments are executed using payment card network technology. These systems are owned and operated by payments network schemes (VISA, MasterCard, China UnionPay etc.). In order to issue pre-paid cards, participants must be "certified" by network schemes. A rigorous technology assessment is conducted of applicant issuer systems prior to network scheme approval. As a result, technology risk for pre-paid cards is driven primarily by circumstances within each country (e.g., system outages due to national utility infrastructure failures or limitations of national payments systems).

Pre-paid card payment methods are also susceptible to technology risk through hardware exploitation. The most popular form of this is called "skimming", where the criminal appends a piece of hardware to an ATM or POS device that duplicates and saves the confidential card details. These details are then used to create a replica card that can be used to embezzle funds.

Finally, pre-paid cards payments are also vulnerable to cyber-crime. In this instance, cyber-criminals attack network systems through the internet with the objective of stealing confidential payments information. This is considered a lesser risk due to the insulation of the systems on network platforms and the general sophistication of these systems.

#### *Technology Risk Mitigation – Pre-paid Cards*

For pre-paid card payments vulnerable to system outages due to country infrastructure issues, risks can be mitigated by individual institutions through the establishment of disaster recovery programs and the maintenance of independent power facilities and offsite system replication capabilities. This type of emergency contingency planning is a regular part of corporate practice in developed economies.

The risk of fraud through "skimming" has been successfully lowered in developed

economies by the introduction of new technology (e.g., Chip and PIN) using the EMV standard. This technology requires the user to enter a pin number to authenticate every transaction. Cardholder and ATM/POS operator education can also be effective tools in preventing card "skimming". The large networks also operate fraud detection software that tracks patterns to provide early warning fraud alerts. Cards identified using this method are stopped for payments until the issue is investigated and resolved.

### **5.8.4. Mobile Payments**

Mobile payments operate through the telecommunications infrastructure. As such, the effectiveness of this payment method is dependent on both network coverage and functionality. The technology risk associated with both coverage and functionality is network specific and should be evaluated based on the particular circumstances of each individual case (e.g., network infrastructure and country utility infrastructure).

In addition, mobile payments are executed using a variety of payment technologies (e.g., NFC, browser, native payment application, bill to carrier, and message based). These technologies span mobile proximity payments and mobile remote payments and each contains specific risks. These can be categorized into three primary risk groups: hardware risk, software risk, and operating platform risk.

#### *Mobile Remote Payments (Browser, Native Applications, Bill to Carrier, Messaging)*

Hardware technology risk for mobile remote payments is risk associated with the physical elements of mobile devices (e.g., SIM card, SD card etc.). The risk associated with hardware failure is low as the majority of hardware used in mobile devices is established and tested in the consumer environment.

Some software technology risks for mobile remote payments exist. As previously noted this software can take the form of a mobile web-browser, a native application, or a SMS payment. The technology risk is significant as technology security is relatively weak and proven industry security standards do not exist. In addition, mobile web-browsers and native applications store sensitive consumer data and operate weak encryption technology that is vulnerable to cyber-attack. In these instances attackers can target software weaknesses to steal sensitive payment information (e.g., account and security information). SMS payments can also be compromised by baseband attacks, whereby the attacker can access the mobile device through the baseband by replicating a cell tower, also potentially gaining access to sensitive payment information. However, it must be noted that, to date, no mobile payments software breach has resulted in a significant financial loss or a loss of data.

Operating platform technology risk for mobile remote payments is centered on wireless internet and telecommunication networks. Technology risk for these elements is notable as a proven industry standard does not exist and relatively weak encryption can be



## Risk Analysis and Mitigation: *Technology Risk*

exposed to reveal sensitive payment information. Networks are also exposed to authentication weakness often the result of design flaws that allow packet sniffing,<sup>69</sup> Man-in-the-Middle attacks,<sup>70</sup> session hijacking and fake SSL certification. This risk can be greater for users that are often in locations without connectivity. SMS communications are designed to occur in real-time, which helps to reduce exposure to these kinds of attacks. When SMS messages are not received immediately by the intended recipient due to lack of connectedness, there is greater opportunity for the message to be intercepted.

### *Mobile Proximity Payments (NFC technology)*

As above, hardware technology risk for mobile proximity payments is risk associated with the physical elements of mobile devices (e.g., NFC chip, SIM card, SD card etc.). Again, the risk associated with hardware failure is low as the majority of hardware used in mobile devices is established and tested in the consumer environment. NFC communication also utilizes the proven security technology standard EMV. The risk of compromise from cyber-attack is also low. This can take the form of "sniffing" or "listening", where a third party intercepts payments data broadcast via the NFC chip. This is deemed a low risk as the broadcast range and duration of NFC transmissions is short (up to 10 cm and generally 1 second) and listening devices would be visible to the mobile phone user.<sup>71</sup>

Software technology risk for mobile proximity payments is centered on native applications that are downloaded to the mobile device and used as virtual wallets. Technology risks for these elements exist as the applications are not designed to any industry standards and new technologies are unproven in security terms. Tests performed by ViaForensics on the Google wallet application revealed significant weaknesses that allowed the tester to access a significant amount of confidential consumer data housed in the application (e.g., balance, limits, transaction information, PIN numbers).<sup>72</sup> However, to date there has been no significant instance of payments fraud for mobile proximity payments.

Operating platform technology risk for mobile proximity payments is not applicable as neither a wireless network nor a mobile phone network is utilized to execute the transaction.

### *Technology Risk Mitigation – Mobile Payments*

As noted above a significant technology risk for this payment method is derived from the coverage and functionality of the network infrastructure and the country utilities infrastructure. Country utility infrastructure issues can be mitigated by individual

---

<sup>69</sup> A packet sniffer is software that captures data packets as data streams flow across a network, decodes the packet's raw data, showing the values of various fields in the packet, and analyzes its content.

<sup>70</sup> A Man-in-the-Middle attack is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection.

<sup>71</sup> Oracle, An Introduction to Near-Field Communication and the Contactless Communication API, June 2008

<sup>72</sup> Mobile App Security and Payments, ViaForensics. Presented at 2012 Payments Forum

## Risk Analysis and Mitigation: *Reputational Risk*

institutions through disaster recovery programs but these risks need to be individually evaluated based on the specific circumstances of each particular case.

For mobile payments vulnerable to hardware, software, and operating platform technology risk, mitigation can be addressed in various ways by focusing on technology enhancements and user education to reduce vulnerability to loss. Systems processes are being designed/redesigned to avoid storage of sensitive data on mobile devices in applications or in general caches. Any sensitive information stored on mobile devices is encrypted using advanced encryption technology. Applications are increasingly designed to reduce user exposure to risk (e.g., mandatory system auto lock features rather than user defined). In addition, increased system security is implemented (e.g., two factor authentication processes are developed as a standard in new payment transaction applications).

In addition to those listed above, user education activities can be used to mitigate the risk of loss from technology failure. In this case, users are educated to recognize and report incidents of fraud (e.g., phishing attacks) and mandated to change their PIN numbers at regular intervals. In addition, users are regularly reminded of security risk and informed of best practice for guarding sensitive information, SIM cards, and phones. Around-the-clock service support is also provided, where security breaches (e.g., lost / stolen phones) can be reported and cancellation procedures implemented.

### **5.8.5. Relevance to USAID and Implementing Partners**

Though there is no direct ability for USAID to influence technology standards applied across the various payment methods, USAID is in a position to encourage Missions and Implementing Partners to evaluate electronic and mobile payments providers based on the standards and practices that they have put in place with the technology that they use, as well as the degree to which they have identified and documented the unique risk profile of the local environment. Ideally, payment providers will have also established reasonable and logical customer due diligence procedures that will help to mitigate technology risks.

## **5.9. Reputational Risk**

Reputational risk is defined here as risk that damages the image of one of the stakeholders, the mobile systems, the financial system, the mobile systems or a specific product. This can occur as a by-product of other activities or the presence of other risks but it also exists as a risk in its own right, particularly in today's increasingly connected marketplace. For example, if fraud occurs under a program managed by a USAID Implementing Partner that disenfranchises a Payment Beneficiary, it has the potential to reflect on the USAID Mission or USAID Headquarters. In a matter of minutes knowledge of such an occurrence could spread through Payment Beneficiary communities and undermine confidence in the entire process. These risks are interconnected and cannot be dealt with as separate elements. Reputational risk must be managed on an aggregate basis, along with the individual

## Risk Analysis and Mitigation: *Reputational Risk*

processes and risks that contribute to reputational risk.<sup>73</sup>

Payment services reputational risk is driven by recipient expectations regarding the delivery of a service and institutional ability to meet its regulatory and consumer protection obligations. Ultimately, reputational risk is about how USAID is perceived by its stakeholders. Managing reputational risk as part of an overall risk infrastructure is a complicated and difficult task. An example of stakeholders that are affected by reputational risk drivers is shown in Figure 22.

Figure 22: Reputational Risk Drivers by Stakeholder

		Reputational Risk Drivers				
		Financial Risk	Systemic Risk	Legal Risk	Operational Risk	Technology Risk
Stakeholders	USAID HQ	☑	☑	☑	☑	
	USAID Missions	☑	☑	☑	☑	
	USAID Implementing Partners	☑		☑	☑	
	Payment Providers	☑	☑	☑	☑	☑
	Payment Beneficiaries				☑	

Good communication is vital to protect against - and repair - reputational damage. This is particularly important in a crisis when the ability to respond quickly and effectively to a difficult situation can enable an organization to defend and oftentimes enhance its reputation.<sup>74</sup>

### 5.9.1. Cash Payments

The reputational risk associated with cash disbursements is primarily focused on fraud and theft. For example, reputational risk arises when cash disbursements are intercepted and redirected from intended sources through corrupt government or payment partner practices. The Payment Beneficiary may become disenfranchised and the reputation of USAID can be damaged as a result of the incident. The long term impact on the USAID brand through association with corrupt or partners, or partners incapable of mitigating payment risk, can ultimately limit USAID's ability to meet development objectives.

#### Reputational Risk Mitigation – Cash Payments

<sup>73</sup> Deloitte Risk Angles, 2012

<sup>74</sup> Economist Intelligence Unit, Reputation: Risk of Risks, 2005

## Risk Analysis and Mitigation: *Reputational Risk*

In addition to previously described mitigating factors in controlling disbursements to limit fraud and theft, reputational risk can be mitigated by establishing good communication channels. This functions by ensuring that market intelligence is distributed to the appropriate part of the organization in a timely manner. This can then be used to inform decision making processes (e.g., communications initiatives and relationship decisions). As part of good communication infrastructure, organizations with effective risk management programs also train employees to identify and report reputational risk issues as they occur.

### **5.9.2. Electronic Funds Transfer**

Reputational risk associated with the transfer of funds using EFT systems is focused primarily on payment partner selection. The ability of a selected institution to deliver on the agreed terms of service will reflect on the brand and reputation of USAID. The risk associated with a given partner varies based primarily on the honesty of the employees working for the institution and the strength and sophistication of both operating controls and system security in place.

In general, interbank EFT systems are strong, internationally-recognized systems that form part of country payment networks and are regulated by government regulatory authorities, normally a financial services regulatory body or the central bank. The reputational risk associated with these types of systems is low due to strong system security and associated procedural controls. However, intra-bank EFT systems can be proprietary bank systems that can vary significantly in terms of process and system strength and sophistication. The reputational risk associated with this payment type must be evaluated based on the individual circumstances of each institution.

#### *Reputational Risk Mitigation – Electronic Funds Transfer*

Reputational risk from EFT payments is already lower than that of other payment methods due to the presence of strong system security and associated procedural controls at the established system providers. Further mitigation can be achieved through implementation of a rigorous partner selection process, whereby partners are evaluated against best practice operating standards to ensure capability to deliver to agreements in a manner acceptable to USAID.

In addition, exposure to reputational risk caused by failure of the EFT payment method can be mitigated by the establishment of strong communications channels with payments partners and ensuring appropriate response procedures are in place to manage developing situations, including escalation criteria.

### **5.9.3. Pre-paid Cards**

Reputational risk associated with pre-paid cards has a number of distinct elements. These

## Risk Analysis and Mitigation: *Reputational Risk*

can be grouped into: fees, illicit activities, and functionality / partner selection.

As noted previously, pre-paid cards are operated using a fee-based revenue model whereby both the cardholder and the merchant can be charged a fee during the execution of a transaction. These fees are effectively the price for the service. However, unlike the price paid for other goods and services, it is often difficult to discern the exact fee being charged. This can lead to cardholder and merchant dissatisfaction and create ill-will toward the service provider. If the fees are not disclosed, this could cause brand and reputation damage to USAID through association.

Pre-paid cards can also be used for illicit activities such as embezzlement and money laundering. As previously noted, this is due to the relative anonymity associated with this method where cardholder authentication is not required and the size of the card makes it easy to store and carry large quantities of money across borders. This type of activity could cause damage to the product by reducing market confidence in it as a tool and consequently limit its effectiveness for payment disbursement.

There is also reputational risk associated with functionality / partner selection for this payment method. As most of the operators in this space are large global corporations this is a lesser concern than other risk elements. However, there are a growing number of national network providers (e.g., Australia - EFTPOS, China – China Unionpay, and Canada - Interac) and as an exercise in prudence partner ability to deliver agreed services and partner operating practice standards should be evaluated in the context of potential impact on reputational risk.

### *Reputational Risk Mitigation – Pre-paid Cards*

In order to mitigate the risk associated with existing pre-paid card scheme fee infrastructure, a number of financial services regulators have initiated regulatory reform aimed at increasing transparency and competition in the payments process (e.g., Canadian 2010 Code of Conduct Legislation<sup>75</sup>, U.S. Durbin Amendment<sup>76</sup>, etc.). These regulations impose requirements and standards with regard to fee transparency, contract cancellation policy and network compatibility to prevent technology-driven monopolies. Some countries have established national payments networks as a means of improving stakeholder confidence in the system. For examples, India recently launched the new Rupay network for domestic transactions. A network initiative aimed at increasing merchant participation in the payments system through the provision of transaction services for a flat low cost fee.<sup>77</sup>

To mitigate against reputational risk derived from illicit activities, payment card network

---

<sup>75</sup> Code Of Conduct for the Credit and Debit Card Industry in Canada. [http://www.fin.gc.ca/n10/data/10-049\\_1-eng.asp](http://www.fin.gc.ca/n10/data/10-049_1-eng.asp)

<sup>76</sup> Anisha. The Durbin Amendment Explained. NerdWallet.com. <http://www.nerdwallet.com/blog/banking/durbin-amendment-explained/>

<sup>77</sup> Deloitte Research, 2012

## Risk Analysis and Mitigation: *Reputational Risk*

schemes are increasing card security through the introduction of two-factor identification processes for transaction execution. This has proved an effective deterrent to criminals when applied to other payment card products (e.g., debit and credit chip and PIN). Functionality / partner selection reputational risk mitigation is similar to that described in the EFT section, where a rigorous partner selection process is required to ensure that all approved partners can deliver on agreements in a manner acceptable to USAID.

Finally, similar to other payment methods, the establishment of strong open communications channels is central to reputational risk mitigation. The organization's ability to gather and report potential reputational risk issues as they arise is crucial to developing mitigation plans and appropriately responding to stakeholder concerns. Additionally, efforts to educate Payment Beneficiary populations on the use of and risks associated with pre-paid card payments is an essential element of reputational risk mitigation for USAID and its Implementing Partners.

### **5.9.4. Mobile Payments**

Similar to pre-paid payments the reputational risk factors associated with Mobile payments can be grouped into: fees, illicit activities, and functionality / partner selection.

As previously described, there is no standard fee model for mobile payments. As a result the fees charged to the mobile phone user and merchant are often confusing. This could cause user and merchant dissatisfaction and lead to a loss of confidence in the payment method. If the fees are not disclosed, this could cause brand and reputation damage to USAID through association.

Mobile payments can also be used for illicit activities such as embezzlement and money laundering. This is due to the relative anonymity associated with this method where user authentication is not always required and transactions can be executed remotely. In addition mobile payments are also deemed more susceptible to "smurfing" (the practice of splitting transactions into smaller sums to avoid notice).<sup>78</sup> This type of activity could cause damage to the product by reducing Payment Beneficiary and merchant confidence in the payment system, and consequently limit its effectiveness for payment disbursement. If associated with illegal drugs or terrorist activities these could cause significant brand damage to USAID.

There is also reputational risk associated with functionality / partner selection for this payment method. As many of the operators in this space are large global corporations, such as Vodafone, MTN, this is a lesser concern than other risk elements. However, there are a significant number of national network providers and as an exercise in prudence partner ability to deliver agreed services and partner operating practice standards should

---

<sup>78</sup> Integrity in Mobile Phone Financial Services Measures for Mitigating Risks from Money Laundering and Terrorist Financing, World Bank Paper No. 146, 2008

## Risk Analysis and Mitigation: *Reputational Risk*

be evaluated in the context of potential impact on reputational risk.

### *Reputational Risk Mitigation – Mobile Payments*

Fee issues for mobile payments can be mitigated in the same manner as pre-paid cards where the financial services regulators have initiated regulatory reform aimed at increasing transparency and participation in the payments process. Mobile payments that leverage payments cards will benefit from existing initiatives, aimed at introducing a standard flat rate fee for transactions. However, other forms of mobile payments will require specific regulation. Competition among mobile money providers may also put downward pressure on fees as has been the case with airtime charges.

Reputational risk derived from illicit activities can be addressed through increased technology security (e.g., two-factor identification processes for transaction execution). This has proved an effective deterrent to criminals when applied to payment card products (e.g., chip and pin). In addition, functionality / partner selection reputational risk mitigation is similar to that described in the pre-paid card and EFT sections, where a rigorous partner selection process is required to ensure that all approved partners can deliver on agreements in a manner acceptable to USAID.

Finally, similar to other payment methods, the establishment of strong open communications channels is central to reputational risk mitigation. The organization's ability to gather and report potential reputational risk issues as they arise is crucial to developing mitigation plans and appropriately responding to stakeholder concerns. Additionally, efforts to educate Payment Beneficiary populations on the use of and risks associated with mobile payments and mobile banking is an essential element of reputational risk mitigation for USAID and its Implementing Partners.

#### **5.9.5. Relevance to USAID and Implementing Partners**

Reputational risk is of particular significance to USAID as it considers the selection and implementation of new payments methods. As noted above reputational damage can be caused by failure or even the perception of failure on behalf of USAID or its partners. Reputational risk is a risk in and of itself but also a derivation of the combination of other risks. This means that stakeholder perceptions of USAID can be affected by a large number of diverse and uncontrollable occurrences. Effective management of these to protect reputation is very difficult. However, while difficult, USAID can take action to protect itself, particularly in the execution of the partner selection process. At a global level USAID can support collaboration of partner organizations through communications programs and education. In addition, USAID can seek to leverage the selection process to establish strong communication channels and foster a culture of information exchange. The objective of which is to ensure that it has access to the most accurate information when making response decisions that will ultimately affect stakeholder perceptions.

## 6. EVALUATION OF PAYMENT ALTERNATIVES

As USAID Missions or Implementing Partners evaluate the suitability of payment types for a specific program, multiple factors should be considered. There is no single set of circumstances or criteria that can be leveraged to create a clear and repeatable decision matrix. In addition, as the mobile and electronic payments landscape continues to evolve internationally, the location and timing of individual development programs will combine to create unique circumstances. Therefore, the decision to choose a specific payment type cannot be prescriptive. It can only be informed by an understanding of the potential benefits and risks at multiple levels. Once achieved, individual decision-makers can evaluate payment type selection based on acceptable risk criteria.

This section provides a framework for informing program-level evaluations of payment alternatives. It is written for general applicability and intended to be used in multiple countries, Missions, or program scenarios. It is by design, not prescriptive. However, it is intended to provide guidance to the decision-maker in when evaluating the risks and benefits of a potential payment type.

Generally speaking, decision-makers should seek, first, to understand the environment and payment type options that exist in a given environment, and to determine which payment types will best serve the needs of the Payment Beneficiaries. Once a level of understanding is achieved regarding availability and utility of payment types (in the context of program objectives) payment alternatives can be evaluated against risk factors specific to the environment. The following sections provide a decision tree and framework to support such an evaluation.

### 6.1. Evaluation Process

Figure 23 provides the high level, logical sequencing to be followed in order to fully understand the viability and risk associated with payment alternatives.

Figure 23: Payment Alternatives Evaluation Methodology



This section of the document provides a decision tree for determining which payment types are to be evaluated and a checklist of potential risks and mitigants. Throughout the document, a “guidepost” version of Figure 23 will aid the evaluator in identifying which step of the process they are currently addressing. The first step in this process is to identify payment type options for evaluation.

### 6.2. Step 1 – Identify Payment Type Options

Before understanding the risks associated with a payment 



## Evaluation of Payment Alternatives: *Step 1* . Identify Payment Type Options

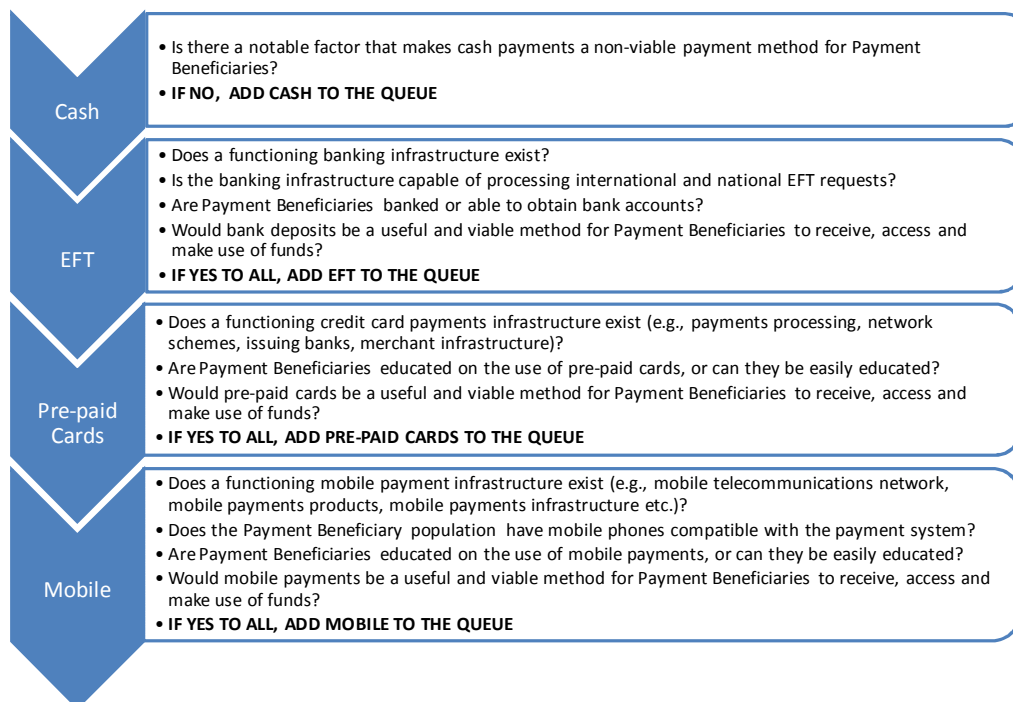
type for a specific program, it is necessary to first assess availability and utility of payment alternatives.

- **Availability** is defined as the presence of a particular payment type within a geography or market in which the USAID program is operating, and that encompasses the Payment Beneficiary population.
- **Utility** refers to the value and practical usefulness of a payment type to the program’s Payment Beneficiaries. This includes the level of comfort and education Payment Beneficiaries have with the payment type, as well as the strength of the overall ecosystem for the payment method.

Availability and utility are equally important factors in determining whether a payment alternative should be considered for use on a USAID program. For example, a target country may have mature mobile payments system in place, with multiple competitors and strong regulation. However, if the Payment Beneficiary population is out of range of a mobile network tower, or if Payment Beneficiaries need to use funds to make purchases from a vendor that does not accept mobile payments, mobile payments are not really a viable option for consideration.

Figure 24 provides a decision tree to guide the evaluator in selecting payment types for evaluation. For each payment alternative, there is a short list of initial screening questions to help determine if that payment type is both available and useful. If the payment alternative is determined to meet both criteria, it should be added to the evaluation queue.

Figure 24: Payment Type Evaluation Decision Tree



## Evaluation of Payment Alternatives:

### 6.3. Step 2 – Determine Risk Profile for Applicable Payment Types

Once the queue for evaluation is complete, the evaluator will use each of the corresponding payment type evaluation tables in the following sections to determine associated risks.



#### 6.3.1. Risk Rating

Each section provides a specific set of risks as well as three levels of potential mitigants or current states that the evaluator will use to rate or “score” a specific payment type. Depending upon the specific risk, the mitigant or current state may not be addressable by the evaluator. For example, if there is risk with respect to the regulatory environment and the current state provides for weak amount of mitigation, it may be beyond the control of the evaluator to directly mitigate. Conversely, if there is risk associated with mobile penetration rates, it may be possible for the evaluator to directly impact the rating by providing mobile phones to the Payment Beneficiaries. The ability of the program actors to influence risk factors by supplying mitigants should be considered during evaluation.

#### 6.3.2. Risk Weighting

In addition to scoring a risk factor as having weak, acceptable or strong mitigants, evaluators should consider the weighting of each factor based on the importance and relevance to the program. Specifically, weighting should be based on the likelihood that a factor will affect program activities, as well as the magnitude of the possible impact to the program associated with that risk factor.

- **Likelihood** – The probability that a risk will be relevant to a program’s funds disbursement activities. Factors that should be taken into account in the determination of likelihood include the source of the potential risk, the ability to influence the source, the nature of program vulnerability and existence and effectiveness of current controls. Likelihood can be rated high, medium and low.
  - **High** – Risk factor is relevant in most circumstances
  - **Medium** – Risk factor is relevant in many circumstances
  - **Low** – Risk factor is relevant in some circumstances
- **Magnitude of Impact** – It is the severity or strength of the effect that a risk could have on the program if it arises. The magnitude of impact can be rated high, medium and low.
  - **High** – Extremely significant impact on Payment Beneficiaries, program operations, reputation, or funding
  - **Medium** – Significant impact on Payment Beneficiaries, program operations, reputation, or funding
  - **Low** – Low impact on Payment Beneficiaries, program operations, reputation, or funding status

## Evaluation of Payment Alternatives:

Likelihood and magnitude of impact together will assist evaluators in determining an overall weight for a given risk factor. Depending on the specificity with which an evaluation is being conducted, this can be done numerically or with just an overall high, medium or low weighting.

It should be emphasized again that value to Payment Beneficiaries should be a primary consideration in risk factor weighting. Creating a more efficient or accountable process to disburse funds at the expense of the Payment Beneficiary is counter to the delivery of effective foreign assistance.

The tables in the following sections should only be completed if the corresponding payment types passed the criteria in Step 1, and are in the evaluation queue. Additionally, as risks will change over time, the tables can be appended by the evaluator to account for either unique environmental concerns or changes since the writing of this document.

### 6.3.3. Evaluating Risk for Cash



The evaluator should complete Figure 25 by checking the corresponding column in each row for the current state. For many of the risk types, the inherent nature of cash makes it difficult to establish “Strong” controls.

Figure 25: Cash Risk Evaluation

Potential Risk	Weak Control or Mitigants	Acceptable Control or Mitigants	Strong Control or Mitigants	Mitigant Rating	Risk Weighting
Payment Preparation	None	Local bank to hold funds sufficient for a designated period of program activity.  Documented guidelines for the kinds of payments.  Procedures and preparations for the secure storage and transportation	N/A		
Pre-disbursement	None	Wire funds into the local Imprest account.  Payment Beneficiaries will be pre-selected, registered and verified for eligibility. If applicable, use a MFI or CTA  Withdraw cash for individual disbursement period and store in secure environment.	N/A		

## Evaluation of Payment Alternatives:

Potential Risk	Weak Control or Mitigants	Acceptable Control or Mitigants	Strong Control or Mitigants	Mitigant Rating	Risk Weighting
Disbursement	None	Avoid personally transporting and disbursing physical currency.  Validate disbursement schedule against Payment Beneficiary registry and verify chain of ownership.  Signed and countersigned registry sheet with receipt.	N/A		
Post Disbursement		Imprest account updated and budget reconciled against disbursement  M&E methodology to verify proper use by Payment Beneficiaries.  Records are maintained for a minimum of 3 years.	N/A		
Theft from Payment Beneficiary	Disbursement of funds in secure environment on a rotating schedule.	N/A	N/A		
AML/CFT	None	Payment Beneficiary pre-screening, validation, and registry. Face to face disbursements.	N/A		

### 6.3.4. Evaluating Risk for Electronic Funds Transfer



The evaluator should complete Figure 26 by checking the corresponding column in each row for the current state. As noted in previous sections, this table should only be completed if EFT has passed the initial screening and added to the queue for evaluation.

Figure 26: Electronic Funds Transfer Risk Evaluation

Potential Risk	Weak Control or Mitigants	Acceptable Control or Mitigants	Strong Control or Mitigants	Evaluator Rating	Risk Weighting
Government / Regulatory Framework					
<ul style="list-style-type: none"> <li>AML/CFT Regulation</li> </ul>	No Regulation	Partial FATF Standards adapted to local requirements	Full FATF Standards adapted to local requirements		

## Evaluation of Payment Alternatives:

Potential Risk	Weak Control or Mitigants	Acceptable Control or Mitigants	Strong Control or Mitigants	Evaluator Rating	Risk Weighting
• Banking Supervision	None	Emerging regulatory supervisory system	Established regulatory and supervisory system		
• Consumer Protection	None	Deposit Insurance	Deposit Insurance Fee and rate regulation Consumer complaints body (e.g., Ombudsman)		
• E-Money Regulation	None	Emerging electronic payment regulation	Mature electronic payment regulation		
• Banking System Stability <sup>79</sup>	Unstable	Emerging	Stable		
<b>Provider Capability</b>					
• Liquidity management (loan : deposit ratios, tier 1 capital reserve ratios)	Not documented	Established liquidity policies but does not comply with relevant international standards	Complies with relevant international standards		
• Internal financial management system	Not documented	Established and documented financial management system but not audited by outside entity	Established and documented financial management system subject to audit by outside entity		
• Record keeping	Not defined	3 years	3 years		
• Internal controls and accountability (e.g., internal audit function)	Not documented	Established and documented internal controls and accountability for oversight of payment system processing, personnel involved in account management but not audited by outside entity	Established and documented internal controls and accountability for oversight of payment system processing, personnel involved in account management subject to audit by outside entity		

<sup>79</sup> Definition: “ A financial system is in a range of stability whenever it is capable of facilitating (rather than impeding) the performance of an economy, and of dissipating financial imbalances that arise endogenously or as a result of significant adverse and unanticipated events.” (Source: International Monetary Fund WP/04/187, IMF Working Paper, October 2004)

## Evaluation of Payment Alternatives:

Potential Risk	Weak Control or Mitigants	Acceptable Control or Mitigants	Strong Control or Mitigants	Evaluator Rating	Risk Weighting
• Accounting records	Not documented	Established and documented policies for creating and maintaining accounting records for at least 3 years but not audited by outside entity	Established and documented policies for creating and maintaining accounting records for at least 3 years subject to audit by outside entity		
• Disbursement processes	Not documented	Documented but not audited by recognized entity	Documented and audited by recognized entity		
• Account opening	Not documented	Locally appropriate KYC / AML process**	Full Bank or licensed KYC / AML process		
• Transaction processing	Not documented	Established and documented process for tracking transactions and providing confirmation and individual transaction detail	Established and documented process for tracking transactions and providing confirmation and individual transaction detail subject to audit by outside, entity		
• Dispute resolution	Not documented	Established and documented policies for challenging a transaction and prompt dispute resolution	Established and documented policies for challenging a transaction and prompt dispute resolution subject to audit by outside, entity		
• Clearing and settlement	Not documented	Documented clearing and settlement policies**	Documented and audited clearing and settlement policies		
• Fraud monitoring	Not documented	Documented transaction fraud monitoring polices, including periodic review, mandatory key person vacation, and unusual transaction flagging **	Documented and audited transaction fraud monitoring polices, including periodic review, mandatory key person vacation, and unusual transaction flagging		
• Data privacy and security policies	Not documented	CTIA / PCI DSS Standards**	CTIA / PCI DSS Standards Previously audited		
General Technology Risk					

## Evaluation of Payment Alternatives:

Potential Risk	Weak Control or Mitigants	Acceptable Control or Mitigants	Strong Control or Mitigants	Evaluator Rating	Risk Weighting
<ul style="list-style-type: none"> <li>Stability of service and power network</li> </ul>	Service or power outages common or unpredictable and/or provider has weak or no contingencies	Occasional service or power outages and/or provider has contingencies that reasonably protect customers	Service or power outages are infrequent and provider has strong contingencies		

### 6.3.5. Evaluating Risk for Pre-paid Cards



The evaluator should complete Figure 27 by checking the corresponding column in each row for the current state. As noted in previous sections, this table should only be completed if pre-paid cards have passed the initial screening and added to the queue for evaluation.

Figure 27: Pre-paid Cards Risk Evaluation

Risk	Weak Control or Mitigants	Acceptable Control or Mitigants	Strong Control or Mitigants	Evaluator Rating	Risk Weighting
Electronic Payments Infrastructure	Acceptance at <10% of POS	Issuance and Acceptance for <50% of POS	Issuance and Acceptance for >50% of POS		
Government / Regulatory Framework					
<ul style="list-style-type: none"> <li>AML/CFT Regulation</li> </ul>	No Regulation	Partial FATF Standards adapted to local requirements	Full FATF Standards adapted to local requirements		
<ul style="list-style-type: none"> <li>Banking Supervision</li> </ul>	None	Emerging supervisory system	Established supervisory system		
<ul style="list-style-type: none"> <li>Consumer Protection</li> </ul>	None		Deposit Insurance Fee and rate regulation		
<ul style="list-style-type: none"> <li>E-Money Regulation</li> </ul>	None	Emerging electronic payment regulation	Mature electronic payment regulation		
<ul style="list-style-type: none"> <li>Issuer licensing / registration</li> </ul>	None	Registration Requirement	Licensing Requirement		
Banking System Stability <sup>80</sup>	Unstable	Emerging	Stable		

<sup>80</sup> Definition: “ A financial system is in a range of stability whenever it is capable of facilitating (rather than impeding) the performance of an economy, and of dissipating financial imbalances that arise endogenously or as a result of significant adverse and unanticipated events.” (Source: International Monetary Fund WP/04/187, IMF Working Paper, October 2004)

## Evaluation of Payment Alternatives:

Risk	Weak Control or Mitigants	Acceptable Control or Mitigants	Strong Control or Mitigants	Evaluator Rating	Risk Weighting
<b>Provider Capability</b>					
<ul style="list-style-type: none"> <li>Internal financial management system</li> </ul>	Not documented	Established and documented financial management system but not audited by outside entity	Established and documented financial management system subject to audit by outside entity		
<ul style="list-style-type: none"> <li>Record keeping</li> </ul>	Not defined	1 year	3 years		
<ul style="list-style-type: none"> <li>Internal Controls and accountability (E.g., internal audit function)</li> </ul>	Not documented	Established and documented internal controls and accountability for oversight of payment system processing, personnel involved in account management but not audited by outside entity	Established and documented internal controls and accountability for oversight of payment system processing, personnel involved in account management subject to audit by outside entity		
<ul style="list-style-type: none"> <li>Accounting records</li> </ul>	Not documented	Established and documented policies for creating and maintaining accounting records for at least 3 years but not audited by outside entity	Established and documented policies for creating and maintaining accounting records for at least 3 years subject to audit by outside entity		
<ul style="list-style-type: none"> <li>Disbursement processes</li> </ul>	Not documented	Documented but not audited by recognized entity	Documented and audited by recognized entity		
<ul style="list-style-type: none"> <li>Account opening</li> </ul>	Not documented	Locally appropriate KYC process**	Full Bank or licensed provider KYC process		
<ul style="list-style-type: none"> <li>Transaction processing</li> </ul>	Not documented	Established and documented process for tracking transactions and providing confirmation and individual transaction detail	Established and documented process for tracking transactions and providing confirmation and individual transaction detail subject to audit by outside, recognized entity		
<ul style="list-style-type: none"> <li>Dispute resolution</li> </ul>	Not documented	Established and documented policies for challenging a transaction and prompt dispute resolution	Established and documented policies for challenging a transaction and prompt dispute resolution subject to audit by outside, recognized entity		
<ul style="list-style-type: none"> <li>Clearing and settlement</li> </ul>	Not documented	Documented clearing and settlement policies**	Documented and audited clearing and settlement policies		



## Evaluation of Payment Alternatives:

Risk	Weak Control or Mitigants	Acceptable Control or Mitigants	Strong Control or Mitigants	Evaluator Rating	Risk Weighting
<ul style="list-style-type: none"> <li>Fraud monitoring</li> </ul>	Not documented	Documented transaction fraud monitoring polices, including periodic review, mandatory key person vacation, and unusual transaction flagging**	Documented and audited transaction fraud monitoring polices, including periodic review, mandatory key person vacation, and unusual transaction flagging  Also includes predictive modeling capability to identify fraud patterns		
<ul style="list-style-type: none"> <li>Data privacy and security policies</li> </ul>	Not documented	CTIA / PCI DSS Standards**	CTIA / PCI DSS Standards  Previously audited		
<ul style="list-style-type: none"> <li>Agent governance and monitoring</li> </ul>	Not documented	Established and documented policies for agent governance	Documented and audited for policy compliance		
<ul style="list-style-type: none"> <li>Agent selection process</li> </ul>	Not documented	Established and documented process for agent selection	Documented and previously audited for policy compliance		
<ul style="list-style-type: none"> <li>Agent reporting</li> </ul>	Not documented	Established and documented policies for reporting by agents to ensure integrity of transactions and performance	Documented and previously audited for policy compliance		
<b>General Technology Risk</b>					
<ul style="list-style-type: none"> <li>Stability of service and power network</li> </ul>	Service or power outages common or unpredictable and/or provider has weak or no contingencies	Occasional service or power outages and/or provider has contingencies that reasonably protect customers	Service or power outages are infrequent and provider has strong contingencies		

## Evaluation of Payment Alternatives:

### 6.3.6. Evaluating Risk for Mobile



The evaluator should complete Figure 28 by checking the corresponding column in each row for the current state. As noted in previous sections, this table should only be completed if mobile has passed the initial screening and added to the queue for evaluation.

Figure 28: Mobile Payments Risk Evaluation

Potential Risk	Weak Control or Mitigants	Acceptable Control or Mitigants	Strong Control or Mitigants	Evaluator Rating	Risk Weighting
Mobile Penetration	< 50%	>50%	>80%		
Government/Regulatory Framework					
• AML/CFT Regulation	No Regulation	GSMA standards adapted to local requirements	Full FATF Standards adapted to local requirements and risk environment		
• Banking Supervision	None	Emerging supervisory system	Established supervisory system		
• Consumer Protection	None	Segregated accounts for mobile money held in bank or trust accounts	Bank Deposit Insurance Fee and rate regulation		
• E-Money Regulation	None	Emerging electronic payment regulation	Mature electronic payment regulation		
• Agent licensing / registration	None	Registration Requirement	Licensing Requirement		
Banking System Stability <sup>81</sup>	Unstable	Emerging	Stable		
Provider Capability					
• Internal financial management system	Not documented	Established and documented financial management system but not audited by outside entity	Established and documented financial management system subject to audit by outside entity		
• Record keeping	Not defined	1 year	3 years		

<sup>81</sup> Definition: “ A financial system is in a range of stability whenever it is capable of facilitating (rather than impeding) the performance of an economy, and of dissipating financial imbalances that arise endogenously or as a result of significant adverse and unanticipated events.” (Source: International Monetary Fund WP/04/187, IMF Working Paper, October 2004)

## Evaluation of Payment Alternatives:

Potential Risk	Weak Control or Mitigants	Acceptable Control or Mitigants	Strong Control or Mitigants	Evaluator Rating	Risk Weighting
• Internal Controls and accountability	Not documented	Established and documented internal controls and accountability for oversight of payment system processing, personnel involved in account management but not audited by outside entity	Established and documented internal controls and accountability for oversight of payment system processing, personnel involved in account management subject to audit by outside recognized entity		
• Accounting records	Not documented	Established and documented policies for creating and maintaining accounting records for at least 3 years but not audited by outside entity	Established and documented policies for creating and maintaining accounting records for at least 3 years subject to audit by outside entity		
• Internal controls that comply with local laws	Not documented	Established and documented internal control policies for compliance with local laws but not audited by outside entity	Documented and audited by outside entity		
• Reporting and records maintenance	Not documented	As required by local law and accounting standards and for at least 1 year -	As required by local law and accounting standards and for at least 3 years- and subject to audit by outside entity		
• Disbursement processes	Not documented	Documented but not audited by outside entity	Documented and audited by outside entity		
• Account opening	Not documented	Locally appropriate KYC process**	Full Bank or licensed provider KYC process		
• Transaction processing	Not documented	Documented process for tracking transactions and providing confirmation and individual transaction detail**	Documented and previously audited		
• Dispute resolution	Not documented	Established and documented policies for challenging a transaction and prompt dispute resolution	Established and documented policies for challenging a transaction and prompt dispute resolution and subject to audit by outside entity		

## Evaluation of Payment Alternatives: /Step 3 . Decide on Suitable Level of Risk

Potential Risk	Weak Control or Mitigants	Acceptable Control or Mitigants	Strong Control or Mitigants	Evaluator Rating	Risk Weighting
• Clearing and settlement	Not documented	Documented clearing and settlement policies**	Documented and audited clearing and settlement policies		
• Fraud monitoring	Not documented	Documented transaction fraud monitoring polices, including periodic review, mandatory key person vacation, and unusual transaction flagging**	Documented and audited transaction fraud monitoring polices, including periodic review, mandatory key person vacation, and unusual transaction flagging		
• Data privacy and security policies	Not documented	CTIA / PCI DSS Standards**	CTIA / PCI DSS Standards Previously audited		
• Agent governance	Not documented	Established and documented policies for agent governance**	Documented and previously audited		
• Agent selection process	Not documented	Established and documented process for agent selection **	Documented and previously audited		
• Agent reporting	Not documented	Established and documented policies for reporting by agents to ensure integrity of transactions and performance **	Documented and previously audited		
• Interoperability	No standards or switch	Standards defined	Emerging interoperability in country		
• Alternative Access to Funds by Entity Other than Provider	No alternative access	Alternative access enabled	Alternative access enabled at same cost		
<b>General Technology Risk</b>					
• Stability of service and power network	Service or power outages common or unpredictable and/or provider has weak or no contingencies	Occasional service or power outages and/or provider has contingencies that reasonably protect customers	Service or power outages are infrequent and provider has strong contingencies		

### 6.4. Step 3 – Decide on Suitable Level of Risk



Once the evaluator has completed the payment type evaluations, a decision must be made at the program level regarding risk tolerance. Risk tolerance is the level of risk the program

## Evaluation of Payment Alternatives: /Step 4 . Evaluate Cost Efficiency

is willing to take on related to disbursement of funds to Payment Beneficiaries. There are multiple possible drivers of risk tolerance including, but not limited to:

- Program prioritization of financial inclusion
- Specific objectives for the Payment Beneficiary population that rule out certain payment types
- Environmental conditions that cause the program to prioritize speed of response
- Level of comfort with a payment type among program administrators or Payment Beneficiaries

In Step 2 of the evaluation process, evaluators are given the option of weighting risk criteria and sub-criteria. By lowering the weights of higher risk criteria, it would be possible to produce a lower average risk that is not fully representative in order to avoid separately documenting a risk tolerance justification. A more useful evaluation process includes both realistic risk weighting and assessment, examined in the context of program-level risk tolerance.

After the evaluator has completed the tables for each of the payment types in the queue, there will be a corresponding amount of “Strong”, “Acceptable”, and “Weak” ratings for controls and mitigating factors for each of the risks, as well as a determination of weight based on likelihood and magnitude. The aggregate risk should be considered, qualitatively, against risk tolerance.

### 6.5. Step 4 – Evaluate Cost Efficiency



After Payment Beneficiaries, providers, and the governmental/regulatory environment are evaluated, the final step is to understand whether or not a specific payment type is an efficient and effective means by which to spend U.S. taxpayer dollars. Evaluators should consider the total incremental cost of disbursement for each payment alternative, including payment transaction cost factors that may decrease the per dollar disbursement percentage to the Payment Beneficiary, as well as opportunity costs to the program in the form of lost productivity or efficiency. The latter cost element is likely to be difficult to determine with any degree of specificity, but to the extent possible the incremental burden on program operations should be considered.

Transactions costs are fees to which an individual payment transaction may be subject, and which may be imposed on the sender, the recipient or both. In Step 2, the risks of unknown or variable transaction costs were evaluated. In this section, evaluators should consider all known costs of payment alternatives as part of the overall evaluation process. These costs will vary by payment type:

- Transaction costs for cash include any monetary fee and cost of personnel and equipment involved in the acquisition, transportation, or disbursement of physical currency.

## Evaluation of Payment Alternatives: *Moving Forward*

- Transaction costs for EFT are typically a straightforward fixed fee per transaction. Payment recipients’ banks will often charge a fee to receive the funds and to disburse them to the Payment Beneficiary.
- Pre-paid cards can carry transaction costs to both the consumer and to the merchant where cards are used. In situations where cards are loaded by one funding entity to benefit many (e.g. disbursement of monthly benefits) there may also be fees and charges to the funding entity.
- Transaction costs for mobile payments are not yet standardized, but successful providers (such as M-Pesa) have implemented a fairly transparent tiered fee structure based on the amount of funds being transferred. The fee is typically incurred by the sender of funds.

Figure 29 below is intended to apply to any payment type that made it into the evaluation queue and was analyzed for risk.

Figure 29: Cost Efficiency Evaluation

Cost Factor	Weak Control or Mitigants	Acceptable Control or Mitigants	Strong Control or Mitigants	Evaluator Rating	Risk Weighting
Administrative	Requires significant and manual either logistical or administrative support in order to execute a payment.	Some automation of payment process	Payment process is mostly automated and requires limited manual intervention.		
Sender costs	Not disclosed	Clearly disclosed	Clearly disclosed and competitive		
Recipient costs	Not disclosed	Clearly disclosed	Clearly disclosed and competitive		
Productivity opportunity cost	Disbursements cannot be executed without significant dedicated time and staff	Disbursements do not require additional dedicated staff but take significant time away from other program activities.	Disbursements can be accomplished with minimal additional level-of-effort from existing staff		

### 6.6. Moving Forward

As USAID Missions and Implementing Partners evaluate their unique environments against this transition guidance, it may be the case the current state provides the only acceptable level of risk. However, either programmatic or administrative goals may be encouraging the transition toward another payment type, such as mobile or electronic. In the event this occurs, the following list comprises representative examples of actions that may positively affect the risk landscape:

- **Partnerships and Collaborations** – USAID Missions and Implementing Partners may engage with other members in the payments ecosystem, such as an MNO, commercial bank, or central bank to pilot novel payment efforts. The terms of the

## Evaluation of Payment Alternatives: *Moving Forward*

partnership should include fallback provisions for all parties involved so that in the event a systemic failure occurs, the Payment Beneficiaries are not left without payment. Additionally, provisions may include extra audit, insurance, or infrastructure requirements. The use of these collaborations provides a relatively lower risk profile and allows for experimentation to prove longer term viability.

- **Regulatory Strengthening or Evolution** – Local regulatory bodies and government entities may respond to the market and modify local regulations to include consideration of electronic and mobile payment types. If this occurs it could significantly impact the risk assessment for a relevant program
- **Change in Competitive Landscape** – If additional electronic or mobile payments providers enter the market (or if existing entities begin providing mobile payments services), it could significantly alter the quality and cost of payments services. Of particular note would be if an established payments provider from another market – one that had already adopted established industry standards – it could potentially shift the quality of the entire market.

**APPENDIX A: SUPPLEMENTAL INFORMATION**

**A.1. Regulatory Environment**

**USAID Automated Directives System (ADS) Chapters 549, 625, 630, 636, 22 CFR82 Part 226, OMB83 Circular A-133, Guidelines for Financial Audits Contracted by Foreign Recipients**

Offices with responsibility for funds disbursement, which include USAID Mission Controllers, the Bureau for Management, Office of the Chief Financial Officer, Cash Management and Payments division, are required to maintain appropriate internal controls to process payments in the correct amounts payable to the proper vendors within the specific timeframe established by the Prompt Pay Regulations.

**ADS Chapter 549**

Financial Audit Requirements Chart<sup>84</sup>

CATEGORY	AUDIT THRESHOLD	AUDIT FREQUENCY	COMMENTS
Foreign-Based Contractors	Incurred Costs	Annual assessment (recipient's fiscal year) to determine when to audit	--Prime or subrecipient --ADS 591.3.2.1 and Inspector General Guidelines
Foreign-Based Grantees (Recipient-Contracted Audits)	\$300,000 or more expended in USAID awards	Annual (recipient's fiscal year)	--Prime or subrecipient --Monitor or audit <\$300K --ADS 591.3.2.1 and Inspector General Guidelines
Host Government Entities	\$300,000 or more expended in USAID awards	Annual (recipient's fiscal year)	--Audits may be by Supreme Audit Institution if USAID concurs. --ADS 591.3.2.1 and Inspector General Guidelines
Host Country Contractors and Grantees	\$300,000 or more expended in USAID awards	Annual (recipient's fiscal year)	--Bureau for Management/Office of Acquisition and Assistance arranges for audits of costs claimed under cost-reimbursable contracts/subcontracts awarded to U.S.-based firms. --ADS 591.3.2.1 and Inspector General Guidelines
Host Country-Owned Local Currency Special Accounts	\$300,000 or more expended in USAID awards	Periodic	--Discuss requirements with host governments. --Indicate audit responsibilities, frequency, and funding in assistance objective agreements. --ADS 591.3.2.2
Cash Transfers and Other Awards	\$300,000 or more expended in USAID awards	Annual	--Review or audit. --Use Inspector General Guidelines if appropriate. --591.3.4.2
U.S.-Based Grantees (Recipient-Contracted Audits)	*\$500,000 or more expended in Federal awards	Annual (recipient's fiscal year)	--OMB Circular A-133
U.S.-Based Contractors	Incurred Costs	Annual assessment (recipient's fiscal year) to determine when to audit	--Audits generally conducted by the Defense Contract Audit Agency. --FAR 52.215-2 and 52.216-7

**ADS Chapter 625**

<sup>82</sup> CFR stands for Code of Federal Regulations  
<sup>83</sup> OMB stands for Office of Management and Budget  
<sup>84</sup> <http://www.usaid.gov/policy/ads/500/591saa.pdf>



## Appendix A: Supplemental Information: A.1. Regulatory Environment

ADS Chapter 625 on accounts receivables and debt collection includes debt determinations, proper billing methods and routine servicing of USAID accounts receivables. This section links the electronic paper check conversion to the U.S. Treasury Automated Clearing House (ACH) system for debit or credit transactions through online applications. Under ADS Chapter 625, collection by Electronic Funds Transfer (EFT) or through the Automated Clearing House (ACH) is the preferred method of receiving funds. The Billing Office must ensure that collection and deposit of funds are made by M/CFO/WFS or cashier offices at overseas locations in a timely manner.

### **ADS Chapter 630**

The ADS Chapter 630 on payables management sets the principles, requirements and procedures that govern the examination, certification, and payment of basic vouchers, claims, and other payment requests between certain entities. The payment relationships covered in this chapter are:

- USAID Headquarters to Contractors
- USAID Headquarters to USAID Missions
- USAID Headquarters or USAID Missions to Direct Contractors
- Prime Contractors and Sub-contractors or local contractors.

Regulations in ADS 630 also speak to direct payments and intra-governmental payments and collections (IPAC). However, the chapter does not clearly articulate the payment process relationship between USAID or contractor and the final Recipient. This is highly relevant to evaluation of electronic and mobile payment types. It indicates that the part of the payment process that is most likely to leverage electronic and mobile payments – contractor or sub-contractor to end recipient – is not addressed by ADS guidelines on payments.

Under direct payments, USAID reimburses the recipient/contractor or host country for eligible expenditures that the recipient/contractor incurs and pays. USAID may use this method of payment with any USAID grant or contract.

The IPAC method of transferring funds between Federal agencies is a component of the U.S. Treasury Government On-line Link Service (GOALS), and is used primarily for funds transfer between Federal agencies. USAID accomplishes payment and collection activity for interagency 632(b) reimbursable agreements between agencies using IPAC for both payment and collection activity. USAID also uses the IPAC system as a method of funds transfer between USAID Missions and USAID/W.

There are four key functional roles involved in the USAID payment process.

## Appendix A: Supplemental Information: A.1. Regulatory Environment

- The CFO periodically reviews USAID disbursement systems to ensure that USAID uses the most effective techniques and procedures.
- The Mission Controllers maintain appropriate internal controls to process payments in the correct amount, payable to the proper vendor and within the timeframe established by Prompt Pay Regulations.
- The COTRs perform administrative approval on all vouchers submitted under USAID direct contracts, host country contracts, and inter-agency agreements. The COTRs will know whether goods or services received conform to what was requested and whether payment is in order.
- The Contract Agreement Officers ensure that USAID include payment terms and when payments need to be made by. This includes electronic funds transfers.

### **ADS Chapter 636**

ADS Chapter 636 on program funded advances discusses payments made as advances such as a letter of credit, direct and special letter of commitment, and bank letter of commitment.

An Agency-issued Letter of Credit (LOC) is an instrument certified by an authorized official of USAID's Bureau for Management, Financial Management (M/FM) that authorizes the recipient to request an electronic draw down (or advance) of funds through the Bureau of Management, Office of Financial Management, Cash Management and Payment Division, Grants and Interagency Billings Team (M/FM/CMP/GIB). LOCs are not issued to non-U.S. organizations organized, located, and operated outside the U.S. unless the organization maintains an account in a U.S. bank able to accept a funds transfer from the U.S. Treasury. LOC financing is available for advance payments where the amount required for advances is at least \$50,000 over the life of the contract or grant and there is a continuing relationship with the organization for at least one year.

A Periodic advance by treasury check, ACH or EFT is an advance when payment is made to the recipient by issuance of a Treasury Check, through the Automated Clearing House (ACH), or by electronic fund transfer (EFT). This method is used when an advance is justified but the conditions for a Letter of Credit (LOC) cannot be met.

### **22 CFR Part 226 - Administration of Assistance Awards to Non-Governmental Organizations**

The Electronic Code of Federal Regulations, Part 226, details the administrative requirements for grants and cooperative agreements awarded by USAID to U.S. institutions of higher education, hospitals, and other non-profit organizations, to U.S. commercial organizations and to subawards thereunder.

## Appendix A: Supplemental Information: A.1. Regulatory Environment

According to this regulation, an award is defined as financial assistance that provides support or stimulation to accomplish a public purpose. Awards include grants, cooperative agreements and other agreements in the form of money or property in lieu of money, by the Federal Government to an eligible recipient.

A recipient is an organization receiving a grant or cooperative agreement directly from USAID to carry out a project or program.

A subaward is defined as an award of financial assistance in the form of money, or property in lieu of money, made under an award by a recipient to an eligible subrecipient or by a subrecipient to a lower tier subrecipient.

A subrecipient is the legal entity to which a subaward is made and which is accountable to the recipient for the use of the funds provided.

### Standards for financial management systems

The standards in 226.21 define requirements for recipient's financial systems, indicating that, in order to be eligible to receive an award from USAID, a recipient must have in place a financial accounting system that meets an established threshold. The subarticles of the regulations specifically require that a recipient's financial management systems provide:

- Records that identify adequately the source and application of funds for federally-sponsored activities. These records shall contain information pertaining to all Federal awards, authorizations, obligations, unobligated balances, assets, outlays, income and interest.
- Effective control over and accountability for all funds, property and other assets. Recipients shall adequately safeguard all such assets and assure they are used solely for authorized purposes.
- Comparison of outlays with budget amounts for each award. Whenever appropriate, financial information should be related to performance and unit cost data.
- Written procedures to minimize the time elapsing between the transfer of funds to the recipient from the U.S. Treasury and the issuance or redemption of checks, warrants or payments by other means for program purposes by the recipient. To the extent that the provisions of the Cash Management Improvement Act (CMIA) (Pub. L. 101-453) govern, payment methods of State agencies, instrumentalities, and fiscal agents shall be consistent with CMIA Treasury-State Agreements or the CMIA default procedures codified at 31 CFR part 205, "Withdrawal of Cash from the Treasury for Advances under Federal Grant and Other Programs."

## Appendix A: Supplemental Information: A.1. Regulatory Environment

- Accounting records, including cost accounting records, which are supported by source documentation.

### Retention and access requirements for record

Article 226.53 of this regulation covers the record retention requirements for recipients of awards. It states that “Financial records, supporting documents, statistical records, and all other records pertinent to an award shall be retained for a period of three years from the date of submission of the final expenditure report or, for awards that are renewed quarterly or annually, from the date of the submission of the quarterly or annual financial report, as authorized by USAID.”

### Closeout procedures

Article 226.71 establishes a term of 90 days for recipients to submit “all financial, performance, and other reports as required by the terms and conditions of the award.”

### **OMB Circular A-133: Audits of States, Local Governments and Non-Profit Organizations**

OMB Circular A-133 establishes guidelines for the performance of audits on public and non-profit entities.

### Audit requirements

Subpart B article 200 lays out the following audit requirements:

(a) Audit required. Non-Federal entities that expend \$300,000(\$500,000 for fiscal years ending after December 31, 2003) or more in a year in Federal awards shall have a single or program-specific audit conducted for that year in accordance with the provisions of this part. “

Subpart B article 220 determines the audit frequency as annual.

### Scope of audit

Subpart E article 500 outlines the scope of the audit:

(a) General. The audit shall be conducted in accordance with GAGAS. The audit shall cover the entire operations of the auditee; or, at the option of the auditee, such audit shall include a series of audits that cover departments, agencies, and other organizational units which expended or otherwise administered Federal awards during such fiscal year, provided that each such audit shall encompass the financial statements and schedule of expenditures of Federal awards for each such department, agency, and other organizational unit, which shall be considered to be a non-Federal entity. The financial statements and schedule of expenditures of Federal awards shall be for the same fiscal year.

(b) Financial statements. The auditor shall determine whether the financial statements of

## Appendix A: Supplemental Information: A.2. Mature Payment Methods

the auditee are presented fairly in all material respects in conformity with generally accepted accounting principles. The auditor shall also determine whether the schedule of expenditures of Federal awards is presented fairly in all material respects in relation to the auditee's financial statements taken as a whole.

(c) Internal control. (1) In addition to the requirements of GAGAS, the auditor shall perform procedures to obtain an understanding of internal control over Federal programs sufficient to plan the audit to support a low assessed level of control risk for major programs.

(d) Compliance. (1) In addition to the requirements of GAGAS, the auditor shall determine whether the auditee has complied with laws, regulations, and the provisions of contracts or grant agreements that may have a direct and material effect on each of its major programs.”

### A.2. Mature Payment Methods

#### **Electronic Funds Transfer Act**

The Electronic Funds Transfer Act is from the Financial Institutions Regulatory and Interest Rate Control Act of 1978 (9). This act defines the rights and responsibilities of EFT consumers and providers. For example, the act: sets limits on the liability of consumers if there are errors in an EFT transaction or if an improperly authorized transaction is executed; establishes the responsibility of consumers for ensuring the security of their EFT accounts and for reviewing statements provided by the financial institutions; establishes requirements for the documentation of an EFT transaction that must be provided to the consumer, including definition of the contents of a receipt provided at the time of a transaction and the timing and content of periodic statements that are issued by the service operator; establishes rules governing the issuance of EFT access devices.

#### **OFAC**

International transfers involving the U.S. are subject to monitoring by the Office of Foreign Assets Control (OFAC), which monitors information provided in the text of the wire to ascertain whether money is being transferred to terrorist organizations or countries or entities under sanction by the U.S. government. If a financial institution suspects that funds are being sent from or to one of these entities, it must block the transfer and freeze the funds.

### A.3. Electronic and Mobile Payments

#### **U.S. Federal and State Regulations**

In Title IV, the law prescribed additional obligations regarding disclosure of account terms, stricter regulation of allowable fees, and protection of consumers from losses associated with expiring cards.

Title V, Section 503 required the Treasury Department to issue regulations in final form

## Appendix A: Supplemental Information: A.3. Electronic and Mobile Payments

implementing the Bank Secrecy Act, regarding the sale, issuance, redemption of international transport of stored value, including stored value cards. The Treasury has since taken up the issue and proposed a rule (the notice period has ended but a final rule has not been published as of the writing of this report). The proposed rule:

- Expands the definition to include tangible pre-paid access devices;
- Limits the application of the expanded definition to tangible pre-paid access
- Establishes that the value of any such pre-paid access device would be determined by the amount of the funds available through the device at the time of physical transportation, mail or shipment into or out of the U.S.; and
- Clarifies that credit cards and debit cards are not a form of monetary instrument for BSA purposes.

Office of the Comptroller of the Currency (OCC): The OCC has also addressed store value cards in OCC Bulletin 2006-34 asking issuers to ensure they adequately inform consumers and disclose:

- How, when and where to use the card
- How to increase the balance
- Whether interest, dividends or other return is paid on the electronic cash
- All fees charged
- Name of issuer and its obligation to redeem the electronic cash
- What happens to abandoned or expired funds
- Where liability lies if a transaction is not properly consummated
- Where, how and when to redeem cash
- Whether customer is protected if card is lost or stolen
- Whether the amount is insured by the FDIC
- How consumers can resolve disputes involving transactions
- Circumstances under which information about transactions may be disclosed to third parties
- When the cards are issued by banks, per the same Bulletin they need to:
- Establish that Cards are Issued by a Federally-Chartered Institution
- Consumer's agreement is with the bank
- Card and disclosures identify the bank as the issuer [advertisements, point-of-sale materials, Terms and Conditions, collateral, card carrier, and agreements with card program partners should all reflect bank as issuer
- Bank establishes and imposes the fees and terms
- Bank controls the net proceeds of the fees
- Bank has financial responsibility to merchants that honor the card (holds the funds)

**FATF – List of Jurisdictions with Strategic Deficiencies with Regard to AML/CFT<sup>85</sup>**

In order to protect the international financial system from money laundering and financing of terrorism (ML/FT) risks and to encourage greater compliance with the AML/CFT standards, the FATF identified jurisdictions that have strategic deficiencies and works with them to address those deficiencies that pose a risk to the international financial system.

<p>Jurisdictions subject to a FATF call on its members and other jurisdictions to apply counter-measures to protect the international financial system from the on-going and substantial money laundering and terrorist financing (ML/TF) risks emanating from the jurisdictions*.</p>
<ul style="list-style-type: none"> <li>• Iran</li> <li>• Democratic People's Republic of Korea (DPRK)</li> </ul>
<p>Jurisdictions with strategic AML/CFT deficiencies that have not made sufficient progress in addressing the deficiencies or have not committed to an action plan developed with the FATF to address the deficiencies**. The FATF calls on its members to consider the risks arising from the deficiencies associated with each jurisdiction, as described below.</p>
<ul style="list-style-type: none"> <li>• Cuba**</li> <li>• Bolivia</li> <li>• Ethiopia</li> <li>• Ghana</li> <li>• Indonesia</li> <li>• Kenya</li> <li>• Myanmar</li> <li>• Nigeria</li> <li>• Pakistan</li> <li>• São Tomé and Príncipe</li> <li>• Sri Lanka</li> <li>• Syria</li> <li>• Tanzania</li> <li>• Thailand</li> <li>• Turkey</li> </ul>

\*The FATF has previously issued Public Statements calling for counter-measures on Iran and DPRK. Those Statements are updated below.

\*\*Cuba has not engaged with the FATF in the process.

**A.4. Risk Analysis and Mitigation**

**PCI DSS Rules**

**Build and Maintain a Secure Network**

- Requirement 1: Install and maintain a firewall configuration to protect cardholder

<sup>85</sup> <http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/documents/fatfpublicstatement-16february2012.html>

## Appendix A: Supplemental Information: A.4. Risk Analysis and Mitigation

data

- Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
- *Protect Cardholder Data*
- Requirement 3: Protect stored cardholder data
- Requirement 4: Encrypt transmission of cardholder data access on open, public networks

### **Maintain a Vulnerability Management Program**

- Requirement 5: Use and regularly update anti-virus software
- Requirement 6: Develop and maintain secure systems and applications

### **Implement Strong Access Control Measures**

- Requirement 7: Restrict access to cardholder data to a by business need-to-know basis
- Requirement 8: Assign a unique ID to each person with computer access
- Requirement 9: Restrict physical access to cardholder data

### **Regularly Monitor and Test Networks**

- Requirement 10: Track and monitor all access to network resources and cardholder data
- Requirement 11: Regularly test security systems and processes

### **Maintain an Information Security Policy**

- Requirement 12: Maintain a policy that addresses information security



## APPENDIX B: SOURCE LIST

### B.1. Overview

1. Officer of the Inspector General. Guidelines for Financial Audits Contracted by Foreign Recipients. February 2009
2. OMB Circular A-133. Audits of States, Local Governments, and Non-Profit Organizations. June 2003.  
<http://www.whitehouse.gov/sites/default/files/omb/circulars/a133/a133.pdf>
3. USAID 22 CFR 226. Administration of Assistance Awards to U.S. Non-Governmental Organizations; Marking Requirements. January 2006.  
[http://www.usaid.gov/branding/final\\_rule.pdf](http://www.usaid.gov/branding/final_rule.pdf)
4. USAID. ADS Chapter 630. Payables Management. November 30, 2011.  
<http://www.usaid.gov/policy/ads/600/630.pdf>
5. USAID. ADS Chapter 625. Accounts Receivable and Debt Collection. December 30, 2011. <http://www.usaid.gov/policy/ads/600/625.pdf>
6. USAID. ADS Chapter 636. Program Funded Advancements. December 21, 2011.  
<http://www.usaid.gov/policy/ads/600/636.pdf>
7. Consultative Group to Assist the Poor (CGAP). Notes on Regulation of Branchless Banking in South Africa. February 2008. <http://www.cgap.org/gm/document-1.9.2320/SouthAfrica-Notes-On-Regulation-Branchless-Banking-2008.pdf>
8. Dr. Ignacio Mas. Mobile Banking for the Poor. June 2010.  
<http://globalwa.org/2010/06/dr-ignacio-mas-on-mobile-banking-for-the-poor>
9. USAID-Office of Innovation and Development Alliances (IDEA). USAID Audit Control Guidance on the Use of Electronic Payments - DRAFT. Mobile Money Audit Trail 11 9 2011.docx
10. Public Policy Review. <http://www.gsma.com/documents/public-policy-annual-review-2009/20260>
11. Consultative Group to Assist the Poor (CGAP). Update on Regulation of Branchless Banking in South Africa. January 2010. [http://www.cgap.org/gm/document-1.9.42404/Updated\\_Notes\\_On\\_Regulating\\_Branchless\\_Banking\\_South\\_Africa.pdf](http://www.cgap.org/gm/document-1.9.42404/Updated_Notes_On_Regulating_Branchless_Banking_South_Africa.pdf)
12. Colin C. Richard. Dodd-Frank, International Remittances, and Mobile Banking: The Federal Reserve's Role in Enabling International Economic Development. Northwestern University Law Review. March 2011
13. U.S. Department of Treasury, Financial Management Service. Supplement to Treasury Financial Manual (TFM) Volume I, Part 4, Chapter 10000: Delegation of Disbursing Authority. December 2009. [http://fms.treas.gov/tfm/vol1/agency\\_self-certification\\_guide\\_v13.pdf](http://fms.treas.gov/tfm/vol1/agency_self-certification_guide_v13.pdf)
14. U.S. Department of State. 4 FAH-2 Disbursing Officer Handbook.  
<http://www.state.gov/m/a/dir/regs/fah/04fah02/index.htm>
15. Denise Dias and Katharine McKee. Protecting Branchless Banking Consumers: Policy Objectives and Regulatory Options.. CGAP. September 2010.

## Appendix B: Source List: B.2. Mature Payment Methods

- <http://www.cgap.org/p/site/c/template.rc/1.9.47443/>
16. Islamic Republic of Afghanistan, Da Afghanistan Bank. Article Two: Money Service Providers Regulation.
  17. The Central Bank of Reserve of the Philippines Circular No. 542. Consumer Protection for Electronic Banking. 2006.  
<http://www.bsp.gov.ph/regulations/regulations.asp?type=1&id=1025>
  18. OFAC. <http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx>
  19. Developing and least developed countries legal framework on e-commerce, digital signatures, e-certification, e-transactions, CAs and RAs, EC-DC project participant countries, Monday, February 26, 2001. <http://www.itu.int/ITU-D/ecdc/activities/legalframeworks/legalrequirements26feb01.pdf>

### B.2. Mature Payment Methods

1. Mark Pickens, David Porteous, and Sarah Rotman. Banking the poor through G2P payments. CGAP and Department of International Development (DFID). <http://www.cgap.org/gm/document-1.9.41174/FN58.pdf>
2. Federal Financial Institutions Examination Council. FFIEC Retail Payments System Examination Handbook. March 2004
3. Capgemini, the Royal Bank of Scotland and EFMA. World Payments Report 2011
4. Blog: Can G2P payments drive financial inclusion. March 15, 2012.  
<http://microfinance.cgap.org/2012/03/15/can-branchless-banking-facilitate-financial-inclusion-for-g2p-recipients/>
5. USAID. Flow of Funds Chart. November 12, 2011
6. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act Of 2001. Public Law 107–56—Oct. 26, 2001. <http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf>
7. Potential USAID-Citi Mobile Finance Partnership. The Power of Connecting the Last Mile. December 9, 2011

### B.3. Electronic and Mobile Payments

1. FDIC GC Opinion No. 8. Insurability of Funds Underlying Stored Value Cards and Other Nontraditional Access Mechanisms. Federal Register Vol. 73, No. 220. November 12, 2008
2. Deloitte, GSMA. Taxation and Growth of Mobile in East Africa.  
[http://www.mobileactive.org/files/file\\_uploads/taxation\\_growth\\_mobile\\_east\\_frica\\_2009.pdf](http://www.mobileactive.org/files/file_uploads/taxation_growth_mobile_east_frica_2009.pdf)
3. Colin C. Richard. Dodd-Frank, International Remittances, and Mobile Banking: The Federal Reserve's Role In Enabling International Economic Development. March, 2011

## Appendix B: Source List: B.3. Electronic and Mobile Payments

4. McKinsey & Company. Inclusive growth and financial security: The benefits of e-payments to Indian society. November 2010.  
[http://mckinseysociety.com/downloads/reports/EconomicDevelopment/epayments\\_benefits\\_to\\_Indian\\_society\\_USD\\_191110.pdf](http://mckinseysociety.com/downloads/reports/EconomicDevelopment/epayments_benefits_to_Indian_society_USD_191110.pdf)
5. Verifone. Payware Mobile and Visa Best Practices.  
[http://www.verifonezone.com/fstore/0a463145bbfccb42\\_-9c93e9\\_1307fabb92e\\_-5004/Visa%20Best%20Practices%20White%20Paper%206%2024%2011.pdf](http://www.verifonezone.com/fstore/0a463145bbfccb42_-9c93e9_1307fabb92e_-5004/Visa%20Best%20Practices%20White%20Paper%206%2024%2011.pdf). June 2011
6. William Jack (Georgetown University) and Tavneet Suri (Mit Sloan). The Economics of M-Pesa. August 2010
7. Developing Mobile Money Eco-Systems (Harvard).  
[http://www.hks.harvard.edu/mrcbg/papers/jenkins\\_mobile\\_money\\_summer\\_008.pdf](http://www.hks.harvard.edu/mrcbg/papers/jenkins_mobile_money_summer_008.pdf)
8. GSMA: What makes for a successful mobile money implementation? Learnings from M-Pesa in Kenya and Tanzania.  
[http://www.ifc.org/ifcext/gfm.nsf/AttachmentsByTitle/Tool6.11.GSMAReport-ComparingMPESAKenyaandM-PESATanzania/\\$FILE/Tool+6.11.+GSMA+Report++Comparing+MPESA+Kenya+and+M-PESA+Tanzania.pdf](http://www.ifc.org/ifcext/gfm.nsf/AttachmentsByTitle/Tool6.11.GSMAReport-ComparingMPESAKenyaandM-PESATanzania/$FILE/Tool+6.11.+GSMA+Report++Comparing+MPESA+Kenya+and+M-PESA+Tanzania.pdf)
9. 10 Things You Thought You Knew About M-Pesa. CGAP. November 22, 2010.  
<http://technology.cgap.org/2010/11/22/10-things-you-thought-you-knew-about-m-pesa/>
10. Haiti Leads in Mobile Payments. Partners in Pre-paid. April 23, 2012.  
<https://www.partnersinpre-paid.com/topics/articles/haiti-leads-in-mobile-payments.html>
11. Mwangi S. Kimenyi. Expanding the Financial Services Frontier: Lessons from Mobile Phone Banking in Kenya. Brookings Institute. October 2009.  
[http://www.brookings.edu/articles/2009/1016\\_mobile\\_phone\\_kimenyi.aspx](http://www.brookings.edu/articles/2009/1016_mobile_phone_kimenyi.aspx)
12. ISACA. Mobile Payments: Risk, Security and Assurance Issues. November 2011
13. The Federal Reserve Bank of Chicago. Improving Security for Remote Payments. Chicago Fed Letter. December 2011
14. Deloitte. Mobile Payments: Risk Management Approach. January 2012
15. Mobile Financial Services and Risk Management. Deloitte. October 2011
16. Mobile Commerce Guide 2011. Sybase
17. Davis, Wright. Mobile Payments 101. Tremaine LLP. June 2011
18. Deloitte. Mobile Payments: A Deloitte Analysis. Managing change in the mobile paymentscape
19. Suzanne Kluckey. Mobile Payments 101: Retail. [www.mobilepaymentstoday.com](http://www.mobilepaymentstoday.com). 2011
20. World Economic Forum and Boston Consulting Group. The Mobile Financial Services Development Report 2011.
21. Haiti Mobile Case Study. <http://mmublog.org/wp->

## Appendix B: Source List: B.3. Electronic and Mobile Payments

- [content/files\\_mf/dalberghmmicasestudyfinal.pdf](#)
22. USAID. Accelerating Mobile Money in Indonesia, an Opportunity Assessment (USAID FS Share/Chemonics). October 2011
  23. World Economic Forum. Galvanizing Support: The Role of Government in Advancing Adoption of Mobile Financial Services. 2012
  24. Deloitte. Emerging Markets Mobile Banking & Payments: Regulatory Approaches. April 2010. [EM Mobile Banking and Payments Regulation](#)
  25. Official Journal of the European Union. Directive 2009/110/EC of the European Parliament and of the Council. On the taking up, pursuit and prudential supervision of the business of electronic money. October 2010.  
<http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:267:0007:0017:EN:PDF>
  26. Timothy R. McTaggart. An Overview of Mobile Payments and Their Regulation. The Banking Law Journal. June 2010.  
[http://www.pepperlaw.com/publications\\_article.aspx?ArticleKey=1813](http://www.pepperlaw.com/publications_article.aspx?ArticleKey=1813)
  27. Lyman, Timothy, Mark Pickens, and David Porteous. Regulating Transformational Branchless Banking: Mobile Phones and Other Technology to Increase Access to Finance. 2008. CGAP Focus Note 43.  
<http://www.cgap.org/p/site/c/template.rc/1.9.2583/>
  28. International Treasury Services (ITS.gov). Financial Management Service (FMS).  
<http://www.fms.treas.gov/itsgov/index.html>
  29. A.K.M Fazlur Rahman , Deputy General Manager. Guidelines on Mobile Financial Services (MFS) for the Banks. DCMPS (PSD) Circular Letter no.11. December 20, 2011
  30. Haiti Case Study: [http://www.ssireview.org/pdf/HMMI\\_-\\_Plugging\\_Into\\_Mobile\\_Money\\_Platforms\\_FINAL.pdf](http://www.ssireview.org/pdf/HMMI_-_Plugging_Into_Mobile_Money_Platforms_FINAL.pdf)
  31. GSMA. The case for global interoperability. [http://mmublog.org/wp-content/files\\_mf/mmu\\_interoperability.pdf](http://mmublog.org/wp-content/files_mf/mmu_interoperability.pdf)
  32. GSMA. Mobile Money Transfer. <http://216.239.213.7/mmt/regulatory-impact.asp>
  33. CTIA. Best Practices and Guidelines for Mobile Financial Services. January 28, 2009.  
[http://files.ctia.org/pdf/CTIA\\_MFS\\_Guidelines\\_BP\\_Final\\_1\\_14\\_09.pdf](http://files.ctia.org/pdf/CTIA_MFS_Guidelines_BP_Final_1_14_09.pdf)
  34. CGAP. Haiti Case Study. [http://www.cgap.org/gm/document-1.9.56287/From\\_Market\\_Opportunity\\_to\\_Sustainable\\_Business\\_Rev.pdf](http://www.cgap.org/gm/document-1.9.56287/From_Market_Opportunity_to_Sustainable_Business_Rev.pdf)
  35. USAID FS Share/Chemonics. FS Series #9: Enabling Mobile Money Interventions: Primer, Diagnostic Checklist and Model Scopes of Work. April 2010
  36. USAID. USAID Mobile Solutions Team Draft. Mobile Money Diagnostic Tool. January 2012
  37. Pepper Hamilton LLP. An Overview of Mobile Payments and Their Regulation.  
[http://www.pepperlaw.com/publications\\_article.aspx?ArticleKey=1813](http://www.pepperlaw.com/publications_article.aspx?ArticleKey=1813). June 18, 2010
  38. Risks and Threats Analysis and Security Best Practices: Mobile 2-Way Messaging Systems. Mobile Payment Forum. May 13, 2003.

#### B.4. Risk Analysis and Mitigation

1. VIA Forensics . appWatchdog Findings: Sensitive User Data Stored on Android and iPhone devices. July 2011
2. Shivani Agarwal, Mitesh Khapra, Bernard Menezes and Nirav Uchat. Security Issues in Mobile Payment Systems. Computer Society of India
3. CALP Research: New Technology Enhancing Humanitarian Cash and Voucher Programming.  
[http://www.cashconference.org/images/03\\_how\\_can\\_we\\_send\\_the\\_money.pdf](http://www.cashconference.org/images/03_how_can_we_send_the_money.pdf)
4. USAID. Mobile Financial Services Risk Matrix. July 23, 2010
5. Bill Gajda . Managing the Risks and Security Threats of Mobile Payments.  
[http://pymnts.com/assets/Lyidian\\_Journal/LyidianJournalMarchRiskSec.pdf](http://pymnts.com/assets/Lyidian_Journal/LyidianJournalMarchRiskSec.pdf)
6. FATF. Anti-money laundering and terrorist financing measures and Financial Inclusion. <http://www.fatf-gafi.org/dataoecd/62/26/48300917>
7. ISACA Emerging Technology Whitepaper. Mobile Payments: Risk, Security and Assurance Issues., November 2011
8. MasterCard. MasterCard Payment Application Data Security Standard (Pa-Dss) Mandate. July 2012
9. Payment Card Industry (PCI), Security Standards Council. Navigating PCI DSS: Understanding the Intent of Requirements.. October 2010
10. MasterCard. MasterCard Rules. December 2011
11. PCI Security Standards: <https://www.pcisecuritystandards.org>
12. MasterCard. Security Rules and Procedures. July 2011
13. U.S. Department of Treasury. <http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx>
14. Best Practices for Mobile Device Banking Security: International minimum security guidelines for mobile device banking applications, ATMIA, ATM Industry Association, page 3.  
[http://www.atmia.com/ClassLibrary/Page/Information/DataInstances/1556/Files/525/Best\\_Practices\\_for\\_Mobile\\_Phone\\_Banking\\_Security\\_-\\_Published\\_version.pdf](http://www.atmia.com/ClassLibrary/Page/Information/DataInstances/1556/Files/525/Best_Practices_for_Mobile_Phone_Banking_Security_-_Published_version.pdf)

#### B.5. Country Specific

1. Consultative Group to Assist the Poor. Notes on Regulation of Branchless Banking in Kenya. January 2010. [http://www.cgap.org/gm/document-1.9.42400/Updated\\_Notes\\_On\\_Regulating\\_Branchless\\_Banking\\_Kenya.pdf](http://www.cgap.org/gm/document-1.9.42400/Updated_Notes_On_Regulating_Branchless_Banking_Kenya.pdf)
2. Loretta Michaels, Accenture Development Partnerships. It's Better Than Cash: Kenya Mobile Money Market Assessment. 2011
3. Kabir Kumar & Yanina Seltzer. Blog: Meanwhile in Brazil...are we there yet? April 21, 2011
4. Kabir Kumar & Yanina Seltzer. Blog: Will Brazil's agents become a channel for a wide range of financial services for the poor? June 14, 2011

## Appendix B: Source List: B.6. Other

5. Global Standard-Setting Bodies and Financial Inclusion for the Poor toward Proportionate Standards and Guidance. <http://www.gpfi.org/sites/default>
6. Branchless Banking in Brazil. [http://www.cgap.org/gm/document-1.9.50801/CGAP\\_Technology\\_Program\\_Country\\_Note\\_Brazil\\_Public\\_Rev.pdf](http://www.cgap.org/gm/document-1.9.50801/CGAP_Technology_Program_Country_Note_Brazil_Public_Rev.pdf). CGAP. December 2010
7. Department of Currency Management and Payment Systems - Bangladesh Bank Head Office. Bangladesh Electronic Funds Transfer Network - Operating Rules. DCMPS Circular No. 09/2010. 25 August 2010
8. Honorable Prime Minister Sheikh Hasina. Bangladesh Post Office - Electronic Money Transfer. March 26, 2010. Network Partner: BanglaLink
9. Dr. Md. Ezazul Islam and Md. Salim Al Mamum. Financial Inclusion: The Role of Bangladesh Bank. Working Paper Series: WP1101. December 2011. Research Department, Bangladesh Bank Head Office, Dhaka
10. Global Partnership for Financial Inclusion. Bringing the Principles to Life. 11 Country Case Studies. 2011

### B.6. Other

1. Bill and Melinda Gates Foundation. Financial Services for the Poor Website. <http://www.gatesfoundation.org/financialservicesforthe poor/Pages/default.aspx>
2. Consumer Financial Protection Bureau (CFPB). Supervision and Examination Manual. October 2011
3. Deloitte Development LLC. Cell me the money: Unlocking the value in the mobile payment ecosystem. 2011
4. Alliance for Financial Inclusion research and work. <http://www.afi-global.org/>
5. Regulatory Framework for Mobile Payments Services in Nigeria. <http://www.cenbank.org/OUT/CIRCULARS/BOD/2009/REGULATORY%20FRAMEWORK%20%20FOR%20MOBILE%20PAYMENTS%20SERVICES%20IN%20NIGERIA.PDF>
6. ITU Manual for Measuring ICT Access and Use by Households and Individuals. (2009 EDITION)
7. U.S. Treasury Agency Self-Certification Guide