

E-TRANSFERS IN EMERGENCIES: IMPLEMENTATION SUPPORT GUIDELINES



E-TRANSFERS IN EMERGENCIES:

IMPLEMENTATION SUPPORT GUIDELINES

KOKOÉVI SOSSOUVI

About the author

Kokoévi Sossouvi is an independent consultant specialised in market-based interventions and e-payments. She has extensive experience managing relief programmes in emergency contexts for aid agencies in Asia, Africa and the Caribbean as well as designing mobile solutions for humanitarian interventions for mobile network operators.



TABLE OF CONTENTS

About the author	1
Acknowledgements	5
Glossary of key terms and acronyms	6
Introduction	8
Background to the use of cash in emergencies and the emergence of e-transfers	8
Intended audience	9
Limitations of the guidelines	9
How to use these guidelines	9
SECTION A: Types of e-transfers mechanisms	11
1. Cards	13
2. Mobile transfers	17
3. E-vouchers	21
4. Benefits & drawbacks of e-transfer systems	23
5. In-house/custom-made technology	26
6. E-transfer ecosystems	28
SECTION B: Choosing e-transfer mechanisms	31
1. Getting started with e-transfers	33
2. Assessment checks for e-transfers	36
3. Preparedness and contingency planning	40
4. Beneficiary preferences and protection	43
5. Partnering with service providers	45
6. Cash transfer regulatory issues and beneficiary registration	48
SECTION C: Using e-transfer mechanisms	50
1. Implementation skills	52
2. Beneficiary training and ensuring access by vulnerable groups	53
3. Making e-transfers	55
4. Mitigating fraud risks and dealing with errors	59
SECTION D: Compliance, Monitoring and Evaluation, Data Protection and Complaints	60
1. Compliance	62
2. Programme design, monitoring and evaluation	63
3. Data protection	64
4. Complaints mechanism	66
SECTION E: Additional guidance	67
1. Cash transfer programming reference document	68
2. Procurement process for an e-transfer service provider	69
3. Prerequisites for selecting an e-transfer service provider	70
4. Cash emergency preparedness risk assessment	71
5. Sample mobile usage and awareness questionnaire	72
6. Interview guide/checklist of key issues with service providers	74
7. Minimum contract requirements with an e-transfer service provider	76
8. Fraud and corruption risk mitigation template	77
9. Sample post distribution monitoring (PDM) tools	78
10. Beneficiary Notice and Consent (Plain Language template)	79
11. Data Protection Model Clauses/Aid agency and e-transfer service provider	81
12. Data Protection principles	86

BOXES

Box 1:	ACF food vouchers with Philippines Veterans Bank/Visa (The Philippines)	14
Box 2:	UNHCR cash assistance to refugees with Cairo Amman Bank (Jordan)	15
Box 3:	SOS Children's Villages cash grants with sQuid (Kenya)	16
Box 4:	Wari (West Africa)	17
Box 5:	CARE/CRS mobile vouchers using MerchantPRO by Transversal (Haiti)	19
Box 6:	Concern Worldwide unconditional cash transfers using Zap/Airtel (Niger)	20
Box 7:	Mercy Corps e-vouchers with VoucherPRO by Transversal (Nepal)	22
Box 8:	WFP SCOPe digital platform for cash and vouchers (Global)	26
Box 9:	Oxfam America cash preparedness plan (Senegal)	37
Box 10:	CaLP cost-effectiveness research (Global)	38
Box 11:	NetHope costing tool (Global)	39
Box 12:	Oxfam GB cash grants with UBL (Pakistan)	41
Box 13:	WFP/ACF unconditional mobile transfers with MTN (Côte d'Ivoire)	44
Box 14:	OpenRevolution (US)	46
Box 15:	Banque de la République d'Haïti KYC requirements (Haiti)	49
Box 16:	Mercy Corps picture-based training (Nepal)	54
Box 17:	Concern Worldwide and Safaricom Partnership (Kenya)	55
Box 18:	Sample online interfaces and smartphone applications screenshots (Global)	56
Box 19:	Mercy Corps mobile commerce infographic (Haiti)	58
Box 20:	DRC SMS feedback system (Global)	66

TABLES

Table 1:	Summary features of e-transfer services	23
Table 2:	Benefits and drawbacks of e-transfer mechanisms	24
Table 3:	Minimum requirements for e-transfer systems	28
Table 4:	Range of e-transfer service providers	29
Table 5:	E-transfer planning process	33
Table 6:	Service providers and their associated services	34
Table 7:	Minimum level of service for e-transfer service providers	35
Table 8:	Assessment criteria of e-transfer mechanisms	36
Table 9:	Key elements of an e-transfer service contract	47
Table 10:	Basic e-transfer orientation to request from service providers	52

FIGURES

Figure 1:	Illustrative humanitarian e-transfer ecosystem	30
-----------	--	----

ACKNOWLEDGEMENTS

These *E-transfers in Emergencies: Implementation Support Guidelines* were written for the Cash Learning Partnership (CaLP) (www.cashlearning.org). The guidelines were supported by funding from VISA Inc. and DFID. Please note that the contents of this document are the responsibility of CaLP and do not necessarily reflect the views of DFID or Visa Inc.

The development of these guidelines involved a highly consultative process in which agencies were asked to share their learning and field experience and where possible pilot the draft document. The diverse range of examples provided in this document is a testimony to the support the CaLP has received from its community of practice and is also reflective of the eagerness agencies have to share their learning for the wider benefit of other organisations embarking on what is still a relatively new form of cash transfer. As such, the author and CaLP would like to thank the numerous individuals and organisations that have supported the development of this document.

As part of the consultation process, these guidelines were field tested in Democratic Republic of Congo by Oxfam GB, in Nepal by Mercy Corps, and reviewed by a team who had recently implemented an e-transfer programme, Action Contre la Faim Philippines.

A Technical Working Group was established to support the overall research on e-transfers of which these guidelines form part. The members of the group (listed below) provided input and advice and we would like to take this opportunity to thank them and their organisations for their time, energy and support.

Ruth Aggiss, Save the Children UK

Jenny Aker, Tufts University

Simon Clements, World Food Programme

Olivia Collins, United Nations Children's Fund (formerly with Somalia Cash Consortium)

Hanna Mattinen, United Nations High Commissioner for Refugees

Hamilton McNutt, NetHope

Lili Mohiddin, Cash Learning Partnership

Julien Morel, Action Contre la Faim

Sasha Muench, Mercy Corps

Jessica Saulle, Save the Children UK

Gabrielle Smith, Concern Worldwide

In addition, the following people provided key insights and invaluable comments: Nicholas Leshar (OpenRevolution), Sarah Bailey (Independent Consultant), Sara Murray (Mercy Corps), Jonathan Brass (Oxfam GB), Demos Militante (Action Contre la Faim) and Clare O'Brien (Oxford Policy Management Group) and Fidelis Hove (Oxford Policy Management Group).

Sincere thanks are also extended to the entire CaLP team as well as the CaLP Community of Practice for sharing case studies, active participation in online discussions, and suggestions and comments which informed these guidelines. Gratitude is also extended to the Oxford Policy Management (OPM), specifically Clare O'Brien and Fidelis Hove for their support.

Next steps:

The CaLP is keen to receive feedback from the use of these guidelines. Organisations are kindly invited to send their thoughts and share their programme experiences at info@cashlearning.org and join the CaLP discussion group (by using the link on website www.cashlearning.org).

In addition, readers are reminded that there are substantial resources available on the CaLP website, ranging from case studies and reports on the use of new technologies to cash transfer programme (CTP) guidelines, research on the use of CTP, and market analysis.

GLOSSARY OF KEY TERMS AND ACRONYMS

The key terms frequently used in these guidelines are defined below. Since these terms are not highlighted in the text, readers are invited to frequently refer back to this glossary to seek definitions.

Agent	An entity or retail outlet where an e-transfer can be redeemed for cash.
Agent-merchant	A merchant who provides the services of an agent (see above) in addition to accepting digital payment for selling goods and/or services (cf. merchant).
ATM	Automatic Teller Machine. A computerised telecommunications device that allows the clients of a financial institution to perform financial transactions without the need for a cashier.
Cash collection point	Any location where cash can be collected such as agents, ATMs, Banks, Microfinance Institutions, etc.
Closed loop system	A system in which the entity that issues the e-transfer device (see below) is also the one which holds the relationship with the transaction points (see below). The e-transfer devices can then only be used within the closed loop system.
Contactless card	A smart card that can be read by a near field communication device (NFC) by being tapped on a PoS terminal or a smartphone which is set up to be a card reader.
Ecosystem	The entire architecture and infrastructure required for an e-transfer system to function including the technology, agents, e-transfer devices, senders, receivers, etc.
E-transfer	Electronic transfer. A form of value transfer which uses an e-transfer device (see below) and relies on digital payment systems.
E-transfer device	Electronic transfer device. The vehicle used to store or process an e-transfer such as a SIM card, e-voucher, magnetic strap card, chip card, etc.
E-voucher	Electronic voucher. A form of e-transfer where purchase transactions are authenticated in the system at the time of purchase over the internet or a mobile data service but not over the mobile network (cf. mobile voucher).
KYC	Know Your Customer. A legal customer due diligence process which requires the provision of identification information on the senders and receivers of cash transfers.
Merchant	A trader who accepts digital payment for the sale of goods and/or services, but does not redeem e-transfers for cash (cf. merchant-agent).
Mobile money	Digital currency which is stored in an electronic wallet on a mobile phone.
Mobile token	A form of mobile transfer used to collect cash but not to make purchases (cf. mobile voucher).
Mobile transfer	A form of e-transfer which occurs over the mobile network.
Mobile voucher	A form of mobile transfer used to collect goods (or services) but not cash (cf. mobile token) where authentication occurs over the mobile network (using USSD or SMS) but not over the internet (cf. e-voucher).



Mobile wallet	An electronic wallet accessible on a mobile phone subscribed to a mobile money service.
MNO	Mobile network operator. A service provider that offers mobile network coverage and related products and services.
PoS	Point of sale terminal. A computerised system which allows the completion of payment transactions.
Magnetic stripe card	A plastic card with a magnetic stripe capable of storing data using tiny iron-based magnetic particles on a band on the card and secured by a PIN, a signature or biometrics to verify the identity of the recipient before granting access to the funds.
SIM	Subscriber identification module. An integrated circuit that securely stores data to identify and authenticate subscribers on mobile telephony devices. The circuit is embedded on a small card, commonly called a SIM card.
Smart card	A plastic card with an embedded chip containing information on the recipient and the benefits to which they are entitled.
SMS	Short Message Service. A text messaging service component of communication systems (web, landlines and mobile). It uses standardised communications protocols to allow two-way exchange of short text messages.
Transaction point	Any location where an e-transfer transaction can be conducted. This is not limited to cash collection but also includes merchant purchases.
USSD	Unstructured Supplementary Service Data. A protocol used by Global System for Mobile Communications (GSM) cellular telephones to communicate with the service provider's computers. USSD messages create real-time open connections, which allow a two-way exchange of a data sequences. This makes USSD more responsive than services that use SMS.

A comprehensive glossary of cash transfer terms is available at:

http://www.cashlearning.org/downloads/resources/tools/calp_ctp_glossary-4-april-2011.pdf

INTRODUCTION

BACKGROUND TO THE USE OF CASH IN EMERGENCIES AND THE EMERGENCE OF E-TRANSFERS

Globally, cash payments to poor people, be they from governments, aid agencies or the private sector are in the order of magnitude of billions according to the Better than Cash Alliance.¹ Meanwhile, the rapid spread of technologies enabling branchless banking and digital payment systems has supported the increased consideration of electronic transfers by aid agencies. Over the last five years alone, the CaLP Cash Atlas recorded 41 electronic transfer programmes worldwide targeted at over 3.3 million beneficiaries in emergency settings.²

Electronic transfers, or e-transfers, are a form of value transfer that relies on digital payment systems. The great many benefits they can realise for aid recipients and aid agencies alike in terms of increased security, convenience, privacy, speed, reduced operational/transaction costs and logistics, etc. have been widely documented.³ Equally, many aid agencies have experienced challenges in implementing e-transfers, including in relation to mobile network coverage and reliability, the presence of e-transfer agents, liquidity constraints and low education levels among beneficiaries. Learning from and responding to these challenges is essential.

The increasing use of e-payments, across all aspects of the economy, from the purchase of goods from retailers to the payment of salaries, has added some \$983 billion in global economic growth from 2008 to 2012. They contributed 0.8% increase in GDP in emerging economies and 0.3% in developed markets, with considerable value derived from higher potential tax revenue, lower cost of handling cash, guaranteed payment to merchants, reductions in the grey economy due to lower unreported cash transactions and greater financial inclusion.⁴

With the aim of supporting this increasing use of e-transfers in humanitarian interventions, the Cash Learning Partnership (CaLP) commissioned a report,⁵ in 2011, highlighting the benefits new technologies can bring to humanitarian programmes as well as some of the challenges which are barriers to more widespread adoption. Building on this previous work, and responding to the increasing interest of its community of practice, in 2013, CaLP launched, a three-component research initiative focused exclusively on e-transfers, to build evidence, capacity and develop standards and tools for the humanitarian sector. This research, which seeks to provide guidance on e-transfer programme implementation; an analysis of the cost effectiveness of e-transfers compared to manual cash transfers and beneficiary data protection advice, includes three publications:

- *E-transfers in Emergencies: Implementation Support Guidelines*
- *Factors Affecting the Cost-efficiency of Electronic Transfers in Humanitarian Programmes*
- *Protecting Beneficiary Privacy: Principles and Operational Standards for the Secure Use of Personal Data in E-Transfer Programmes*

¹The Better Than Cash Alliance is members' organisation which provides expertise in the transition to digital payments to achieve the goals of empowering people and growing emerging economies. <http://betterthancash.org/>

²The Cash Atlas (<https://www.cash-atlas.org>) is a dynamic information sharing platform designed by CaLP. The information contained is not exhaustive but rather an indication of the state of cash transfers globally as indicated by the CaLP community of practice.

³See: USAID (2012) *Standards and Practices Report for Electronic and Mobile Payments*. A report by Deloitte Consulting

⁴Zandi, M., Singh, V. & Irving, J. (2013) *The Impact of Electronic Payments on Economic Growth*. Moody's Analytics

⁵Smith, G., MacAuslan, I., Butters, S. and Tromme, M. (2011) *New Technology Enhancing Humanitarian Cash and Voucher Programming*, a Research Report commissioned by CaLP

INTENDED AUDIENCE

These *E-transfers in Emergencies: Implementation Support Guidelines* are intended for the field practitioners of aid agencies engaged in humanitarian responses incorporating cash transfers to be delivered through digital payment systems as well as their extended teams in management and programme support functions.

Although many agencies have developed their own internal processes and standard operating procedures (SOPs) for cash transfers, these documents do not always include specific guidance on the use of e-transfers and the engagement of the private sector. These *E-transfers in Emergencies: Implementation Support Guidelines*, thus seek to provide a basic understanding of e-transfer systems, propose a framework for evaluating the various e-transfer options available, and offer guidance on how to use these options in the delivery of humanitarian assistance.

LIMITATIONS OF THE GUIDELINES

These *E-transfers in Emergencies: Implementation Support Guidelines* assume prior knowledge of cash transfer programming and focus exclusively on **implementing e-transfers** and do not elaborate on decisions relating to whether or not cash is a viable programme option. Therefore, the programme lifecycle begins with assessing which e-transfer option is best suited to deliver a given cash-based intervention.

For readers seeking more in-depth information on cash transfer programme management in general, a guidance sheet on cash transfer reference documents is provided in [Section E-1](#). Extensive additional material is also available on the CaLP website (www.cashlearning.org).

HOW TO USE THESE GUIDELINES

These *E-transfers in Emergencies: Implementation Support Guidelines* are designed as guidance sheets that can be used as reference documents to enable practitioners to easily access their sections of interest or relevance, yet some elements are cross-referenced throughout the documents.

Specific headings are used to guide the reader:

- **“Key learning points”** open each section, summarising the major learning of the section.
- **“Key elements to consider”** introduce the main issues discussed.
- **“Example from the field”** introduces case study boxes to give field-based illustrations of the issues discussed.
- **“Additional guidance”** introduces specific tools that can be found in [Section E](#).

The online version of these guidelines

If you are reading the online version of these guidelines, clicking on any of the blue links will take you to another page in these guidelines, or to a web page. The table of contents on pages 3 and 4 are all linked to their respective pages. At any point in the document, please click on the ‘C’ in the top left hand corner and this will take you straight back to the contents page.

The guidelines are organised into five sections:

A. Types of e-transfer mechanisms

This section provides a description of the main forms of e-transfers currently used by aid agencies, namely card-based transfers, mobile transfers and e-vouchers. It presents the architecture of e-transfers and required ecosystem, whilst also highlighting the benefits and the challenges each option presents.

B. Choosing e-transfer mechanisms

This section is concerned with helping aid agencies make the decision as to which transfer mechanism(s) introduced in Section A may be most appropriate for their intended programme, considering a range of factors and conditions such as preparedness measures, cost analysis, beneficiary preferences, private sectors partnerships and regulatory concerns.

C. Setting up and using e-transfer mechanisms

This section illustrates the process of setting up and using e-transfer mechanisms by reviewing the implementation skills required, the systems used as well as measures to increase participation of the most vulnerable groups, how to mitigate against fraud and errors and ensure data integrity.

D. Compliance, monitoring and evaluation, data protection and complaints

This section addresses questions of compliance with internal policies, procedures and systems as well as donor and legal requirements when choosing to use e-transfers. Attention is paid to the monitoring and evaluation process as well as ways in which to ensure that beneficiary data is protected and complaints are handled appropriately.

E. Additional guidance

Finally, a number of tools are provided in the annexes to support aid agencies using e-transfers.



SECTION A: TYPES OF E-TRANSFER MECHANISMS



PHOTO: SURAJ SHAKYA

Electronic transfers, or e-transfers, are a form of value transfer that relies on digital payment systems, secured generally by a personal identification number (PIN), a signature, or biometrics. Due to their many benefits, e-transfers are increasingly being considered for humanitarian assistance. Over the last five years, the CaLP Cash Atlas recorded 41 humanitarian e-transfer programmes in 17 countries targeted at over 3.3 million beneficiaries.⁶

This section provides a description of the main forms of e-transfers currently used by agencies, namely **card-based transfers**, **mobile transfers** and **e-vouchers**. It presents the architecture of e-transfers and required ecosystem, whilst also highlighting the benefits and the challenges each option presents.

KEY LEARNING POINTS



- Card-based systems used by aid agencies are generally not linked to a bank account but can be loaded with funds that beneficiaries can access directly via ATMs to collect cash or via PoS terminals to make purchases at registered merchants. Transaction authentication can be done using biometrics which, in some contexts, may offer new opportunities for undocumented beneficiaries to access aid. In others, issues can be experienced such as cultural resistance to providing biometric data and limited transferability of the entitlement to a trusted party for housebound beneficiaries.
- Mobile transfers are a form of e-transfer which occurs over the mobile network. The use of mobile phones for e-transfers significantly reduces the need for additional hardware and equipment (cards, PoS terminals, etc.), all the more so since there is growing mobile phone access worldwide.
- E-vouchers are a form of e-transfer where purchase transactions are authenticated in the system at the time of purchase over the internet or a mobile data service. Because each transaction is authenticated in the system at the time of purchase, less time is spent on reconciliation than with paper vouchers.
- Each e-transfer mechanism comes with benefits and drawbacks. Above all else, the realisation of programme objectives should dictate which e-transfer mechanism should be used. Thus, the importance of the context cannot be overstated.
- The minimum requirements for an e-transfers service to function are a technology software, hardware (e-transfer device), connectivity and user accounts.

⁶The Cash Atlas (<https://www.cash-atlas.org>) is a dynamic information sharing platform designed by CaLP. The information contained is not exhaustive but rather an indication of the state of cash transfers globally as indicated by the CaLP community of practice.

I. CARDS

Card-based systems used by aid agencies do not necessarily need to be linked to a bank account, although they may be. They can be loaded with funds that beneficiaries can access directly via ATMs to collect cash or via PoS terminals to make purchases at registered merchants and can thus be used either for unrestricted cash transfers or for voucher programmes.

Increasingly, a number of biometric options such as fingerprint or retina scans are offered by service providers to meet the needs of undocumented populations and facilitate transactions, in some cases, to the point of eliminating the need for the card all together. Careful attention should be paid to the use of biometric data however. First, there can be cultural resistance on the part of beneficiaries to providing biometric data. Furthermore, biometric options also risk restricting the ability of beneficiaries to allow another person to collect funds on their behalf, if for example, they store the fingerprint record of one person only. This can be problematic when the beneficiary has limited mobility, as may often be the case with targeted cash transfer programmes.

The three main types of cards used by aid agencies are **magnetic stripe cards**, **smart cards** and **contactless cards**.

Magnetic stripe cards

Key elements to consider

What they are and how they work: Magnetic stripe, or magstripe, cards are prepaid plastic cards with a magnetic stripe capable of storing data using tiny iron-based magnetic particles on a band on the card.

Transaction authentication is performed in real time, thus requiring constant network connectivity and electricity supply.

What they require: Magstripe cardholder must provide a signature or a PIN of to authenticate transactions and access their funds. Merchants need to have access to a PoS to process purchase transactions or ATMs need to be made available for cash collection.

Summary features

E-transfer mechanism	Beneficiary equipment	Infrastructure at the transaction point	Application
Magnetic stripe card	Card + signature (+ PIN at ATMs)	Merchant with PoS or ATM	Goods/services + cash

*Example from the field***BOX 1: ACF FOOD VOUCHERS WITH PHILIPPINES VETERANS BANK/VISA (THE PHILIPPINES)**

In response to rapid-onset floods of May 2011, **Action Contre la Faim (ACF)** implemented a cash-based intervention in Cotabato City, in the Autonomous Region of Muslim Mindanao in the Philippines. ACF established a voucher programme with local supermarkets to provide flood-affected residents with essential food and non-food items, and piloted the first humanitarian use of magnetic stripe cards in the Philippines.

Through a partnership with CaLP, Visa Inc. helped ACF establish an arrangement with the Philippines Veterans Bank (PVB) to use magnetic stripe cards as cash vouchers. The commodity and point of sale restrictions on the cards reduced both security threats and the potential for diversion of funds.

Magnetic stripe cards had the advantage of allowing beneficiaries to shop multiple times. They simplified the set-up process because they did not require a special design and, distribution only had to occur once as the cards were reloaded electronically. They skirted the security issues in the area and eliminated the potential for misuse of funds for items not included in the intervention because the cards were programmed to only be valid at selected supermarkets.

On the negative side, the cards cost more than paper vouchers. They prevented unspent funds from being reallocated due to usage limits. Finally, they complicated implementation because of the lack of community awareness about payment cards. A key lesson learned was that the use of new technology needs to be accompanied by training and support to beneficiaries.

Source: ACF (2012) *New Cash Transfer Technologies to Attend to Basic Emergency Needs*. CaLP

Smart cards*Key elements to consider*

What they are and how they work: Smart cards are plastic cards with an embedded chip containing information on the recipient and the benefits they are entitled to.

As with magnetic stripe cards, smart card transactions can often be completed “off-line” without network connectivity, to be uploaded on the system when connectivity is restored.

What they require: Cardholders enter their PIN, write their signature or provide biometric data such as fingerprint or retina scans to verify their identity and access their cash. Merchants need to have access to a PoS to process purchase transactions or ATMs need to be made available for cash collection.

Summary features

E-transfer mechanism	Beneficiary equipment	Infrastructure at the transaction point	Application
Smart card	Card + PIN, signature or biometrics	Merchant with PoS or ATM	Goods/services + cash

*Example from the field***BOX 2: UNHCR CASH ASSISTANCE TO REFUGEES WITH CAIRO AMMAN BANK (JORDAN)**

Since 2008, the **United Nations High Commissioner for Refugees (UNHCR)** has been providing monthly unrestricted cash grants to refugees and asylum seekers in Jordan through a successful private banking partnership with Cairo Amman Bank. In 2013, 14,887 refugees and asylum seekers benefited from the scheme.

Since refugees are not allowed individual bank accounts in Jordan, UNHCR holds a master bank account with multiple users (refugees and asylum seekers). Each month, UNHCR channels funds to the bank and the bank informs refugees by SMS when they can withdraw their e-transfer. The money must be withdrawn in two instalments maximum and the users only have access to their designated part of the master account.

Until 2012, all refugees used traditional smart cards with PIN. Now, newly registered refugees use a retina scanning facility which is offered by the bank to all its customers. This new system eliminates the need for a smart card and a PIN. The transaction is based on the recipient's physical presence at the ATM which is equipped with a retina scanning facility. Once the ATM recognises the customer by scanning his/her retina, the machine displays a screen identical to that displayed when using a smart card and a PIN, offering the beneficiary a number of options such as withdrawing money or consulting his/her entitlements.

During specific focus group discussions held with refugees benefiting from the programme, the vast majority report full satisfaction with the programme including those enrolled in the retina scanning scheme. In addition, the bank overhead costs are minimal, at 1.6% of the total budget.

Source: UNHCR

Contactless cards*Key elements to consider*

What they are and how they work: Contactless cards are essentially smart cards that can be read by a near field communication device (NFC) by being tapped on a PoS terminal or a smartphone which is set up to be a card reader. In most instances, new purpose-built PoS terminals must be deployed to authorise transaction or existing terminals can be retrofitted with an NFC sticker that interacts with the contactless card.

What they require: The "tap and go" functionality of contactless cards is secured by presenting formal ID or requesting PIN entry from cardholders for transactions above a certain limit. Merchants need to have access to a PoS with NFC functionality to process purchase transactions or ATMs need to be made available for cash collection.

Summary features

E-transfer mechanism	Beneficiary equipment	Infrastructure at the transaction point	Application
Contactless card	Card + PIN, signature or biometrics	Merchant with NFC PoS or ATM	Goods/services + cash

*Example from the field***BOX 3: SOS CHILDREN'S VILLAGES CASH GRANTS WITH SQUID (KENYA)**

In 2011, **SOS Children's Villages** Kenya established the sQuid programme with the aim of helping villagers affected by drought and famine to access food in Marsabit, northern Kenya. Each beneficiary household was issued with a contactless card – that worked as a voucher – which was loaded with money every two weeks.

The benefits were structured in such a way that each household's sQuid Card was loaded with two e-wallets. One was a restricted e-wallet from which beneficiaries could purchase food and no other type of goods. The second e-wallet was unrestricted in the sense that the beneficiaries could redeem its value for cash. This unrestricted e-wallet, loaded with less value, gave households access to cash to purchase goods like firewood or gas, which are essential in the preparation of the food obtained through the restricted e-wallet.

A PoS device connected to a back-end system managed by a private company, Paystream, and to sQuid Card over the mobile phone network. This back-end system was a regular merchant card system similar to debit card systems and provided for flexible reporting and card management. Also, the PoS could work off-line and the transactions could be processed later, should network connectivity fail. SOS Children's Villages Kenya made direct payments to the shopkeepers according to reports generated from the card management system.

One key advantage of the system for SOS Children's Villages Kenya was the ability to see the transactions in real time, as they happened.

Source: <http://www.squidcard.com/corporate/AidDistribution.html> and CaLP (2013) *Cost-effectiveness of electronic transfers*. A report by OPM.



PHOTO: ANDY HALL/OXFAM

2. MOBILE TRANSFERS

Mobile transfers are a form of e-transfer which occurs over the mobile network.

The use of mobile phones for e-transfers significantly reduces the need for additional hardware and equipment (cards, PoS terminals, etc.), all the more so since there is growing mobile phone access worldwide. On top of being a vehicle for receiving funds transfers, mobile phones provide a means of two-way communication between the programme team and beneficiaries as well as being a communication device for beneficiaries in their daily lives.

The three main forms of mobile transfers used by aid agencies are **mobile tokens**, **mobile vouchers** and **mobile money**.

Mobile tokens

Key elements to consider

What they are: Mobile tokens are a form of mobile transfer used to collect cash only.

How they work: They are a unique authentication code that can be activated only once to release payment at an authorised agent. This authentication code, known only to the receiver, effectively plays the function of a PIN to unlock cash payment (similar to a Western Union tracking number to receive a money transfer).

What they require: Receivers of mobile tokens must have access to a SIM card and are required to collect the full amount that was sent to them, as residual value cannot be stored on the system. Agents need to have access at least a basic phone to process cash collection.

Summary features

E-transfer mechanism	Beneficiary equipment	Infrastructure at the transaction point	Application
Mobile token	SIM + PIN	Agent with basic phone	Cash

Example from the field

BOX 4: WARI (WEST AFRICA)



Available across West Africa, **Wari** is a service provided by the Senegalese company Cellular Solutions International (CSI). It allows cash transfers with mobile tokens for cash collection at an extensive network of agents ranging from small retail outlets to gas station chains.

To initiate the process, the aid agency makes a bank transfer of funds to Wari (beneficiary amounts plus any fees). The agency is then given access to a secure online interface from which to initiate bulk transfers to beneficiaries. Beneficiaries later receive a notification of the transfer by SMS. To collect their payments, beneficiaries confirm their phone number, the token number and present a government-issued ID (depending on the regulation of the country). The Wari agent enters this token number on their own mobile phone and remits the cash to the beneficiary once the transaction is confirmed. A receipt can be printed from a Bluetooth printer.

This system is particularly suited for unrestricted cash transfers to dispersed communities in urban and peri-urban areas. In rural areas, it may be limited by the number of Wari agents, their liquidity and the quality of the mobile network coverage.

Mobile vouchers

Key elements to consider

What they are: Mobile vouchers are a form of mobile transfer used to buy goods (or services) but not to collect cash.

How they work: They are created on a dedicated software system and redeemed at authorised transaction points using a PIN (known to the beneficiary only).

Unlike with mobile tokens, residual value can be stored on the system, thus giving beneficiaries greater flexibility in terms of the amount they can redeem at a time and the number of purchase transactions they can conduct.

What they require: Recipients of mobile vouchers do not always need to have access to a SIM card but always need to have a mobile voucher number and a PIN to authenticate transactions. Merchants need to have access to at least a basic phone to process purchase transactions.

Summary features

E-transfer mechanism	Beneficiary equipment	Infrastructure at the transaction point	Application
Mobile voucher	SIM* + Voucher number + PIN	Merchant with basic phone	Goods/services

* not always required

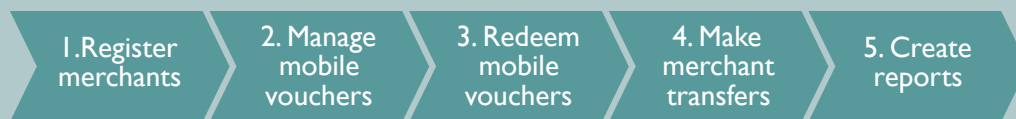


PHOTO: SURAJ SHAKYA

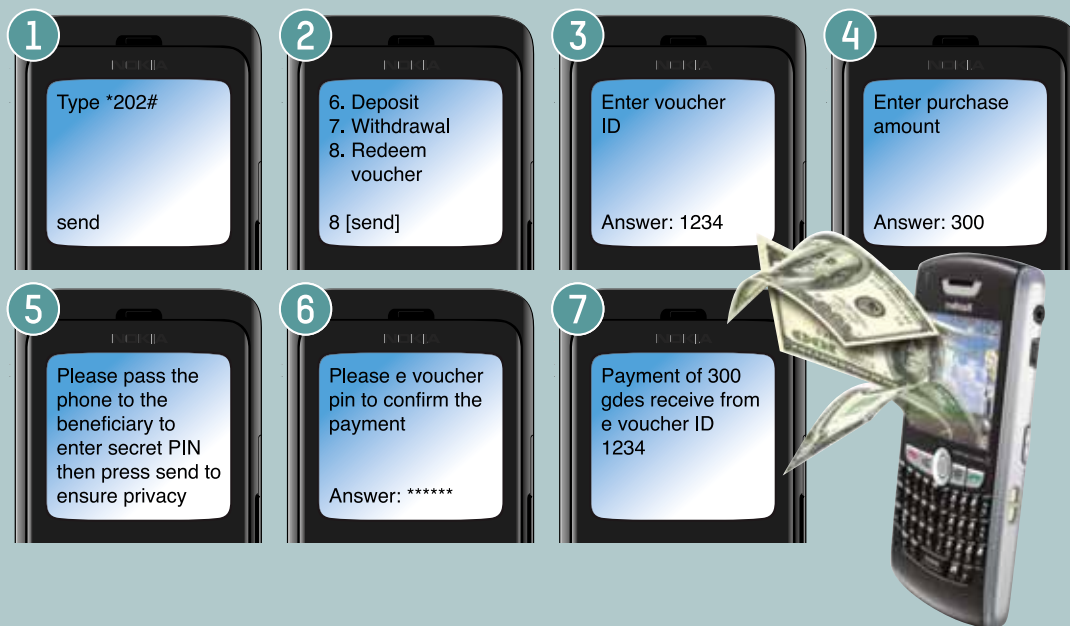
*Example from the field***BOX 5: CARE/CRS MOBILE VOUCHERS USING MERCHANTPRO BY TRANSVERSAL (HAITI)**

In 2012, CARE and Catholic Relief Services (CRS) jointly launched the “Grand’Anse Relief and Recovery Programme (GRRP)” with mobile vouchers created using MerchantPRO, a software platform designed by the Haitian company Transversal. Based on the beneficiary list, vouchers were created in batches and linked to a specific beneficiary ID, which prevented one beneficiary from using another’s voucher.

With beneficiaries receiving a monthly food entitlement to redeem at local stores, the GRPP implementation process included:



Beneficiaries received a mobile voucher code and their PIN on two separate scratch cards. Transactions were authenticated using USSD commands over the mobile network of national operator Digicel, which required beneficiaries to enter their PIN on a merchant’s basic phone, generating the following sequences:



CRS commented that the mobile vouchers reduced cost to 0.60 USD per transaction (versus a paper voucher printed for 5 USD per unit in neighbouring Dominican Republic). In addition, no CRS staff were needed to facilitate transactions. Security agents were not used either. In terms of efficiency, no data entry was required by CRS, as this function was outsourced to Digicel. Finally, data tracking was available online during transactions, which could be made during the entire month.

Despite the success of the programme, the challenges encountered included network connectivity failures which caused delays, as well as a lengthy verification process for merchant payment including triangulation of stock sheets and mobile voucher transactions. Furthermore, many beneficiaries had difficulty remembering and entering their PIN due to limited literacy.

Mobile money

Key elements to consider

What it is: Mobile money refers to the ability to use a mobile phone to conduct financial and commercial transactions such as cash deposit, withdrawal and payments.

How it works: Unlike mobile tokens and mobile vouchers, mobile money requires subscription to a mobile wallet account, where value is stored and which is linked to a specific SIM card or hosted on a technology platform that creates a link (via USSD or SMS) with the mobile handset based on the telephone number.

Mobile money is the most complex form of mobile transfers, and depending on the country and the maturity of the service, the one that can provide recipients with the widest range of transactional capabilities and broader access to basic financial services (such as deposit, withdrawal, person-to-person transfers and e-money transactions with registered traders of goods and service providers).

What it requires: Mobile money users need to have constant access to a phone and to a SIM card that can be linked back to them for the duration of the programme. A PIN is always required to authenticate the mobile money user, grant access to the e-wallet, and initiate transactions. Merchants and agents need to have access to at least a basic phone.

Summary features

E-transfer mechanism	Beneficiary equipment	Infrastructure at the transaction point	Application
Mobile money	Phone +SIM + PIN	Agent/merchant with phone	Goods/services + cash

Example from the field

BOX 6: CONCERN WORLDWIDE UNCONDITIONAL CASH TRANSFERS USING ZAP/AIRTEL (NIGER)



In response to a devastating 2009/2010 drought in Niger, **Concern Worldwide** targeted households in the Tahoua region to receive monthly cash transfers. One-third of targeted households received an e-transfer via the Zap mobile money service offered by the mobile network operator Zain (now Airtel), whereas one-third received manual cash transfers plus a mobile phone and the remaining one-third received manual cash transfers only.

With different beneficiary groups receiving different entitlements, comparisons could be made to understand whether it was the cash transfer, the mobile phone or the mobile transfer that influenced behaviours. The experience showed that the Zap delivery mechanism (using mobile transfer and phone) strongly reduced variable distribution costs for Concern, as well as programme recipients' costs of obtaining the cash transfer.

The Zap approach also resulted in additional benefits: households in Zap villages used their cash transfer to purchase a more diverse set of goods, had higher dietary diversity, depleted fewer assets and grew more types of crops, especially marginal cash crops grown by women. The reasons for this can be attributed to the lower costs and greater privacy of receiving a cash transfer via the Zap mechanism, as well as changes in intra-household decision-making.

This suggests that mobile transfers could be a cost-effective means of providing cash transfers for remote rural populations, especially those with limited road and financial infrastructure.

Source: Aker, J. C., Boumrijel, R., McClelland, A, and Tierney, N. (2011), *Zap It to Me: The Short-Term Impacts of a Mobile Cash Transfer Program*. Center for Global Development

3. E-VOUCHERS

Electronic vouchers, or e-vouchers, are relatively new e-transfer mechanisms used by aid agencies but increasingly being considered as service offerings mature. As with paper vouchers, aid agencies can restrict the type of goods that can be purchased with e-vouchers as well as their retail locations where they can be redeemed – often with efficiency. In addition, beneficiary access is relatively easy as identification requirements to register to an e-voucher system are minimal, compared with other options.

E-vouchers are very similar to mobile vouchers (described above) with the difference that here authentication occurs over the internet (or data service of a mobile network operator), often with the use of a smartphone – and not over the mobile network (via SMS or USSD).

Key elements to consider

What they are: E-vouchers are a form of e-transfer where purchase transactions are authenticated in the system at the time of purchase over the internet or mobile data service.

How they work: They function in a closed loop system, where the entity that issues the voucher (the issuer) is also the one which holds the relationship with the merchant (the acquirer). For example, an aid agency creates e-vouchers (using software licensed from a third party technology provider) and pays the merchants after verification of the vouchers (directly by check/cash or via a financial institution) on an agreed timeframe. In this respect, less time is spent on reconciliation than with paper vouchers because each purchase transaction is authenticated in the system at the time of purchase. This also significantly reduces leakages, as only transactions in the system are valid. These can then be triangulated with the number of beneficiaries registered and the value of their entitlement.

What they require: E-vouchers do not require beneficiaries to have an e-transfer device, such as a mobile phone. Beneficiaries need only have a voucher number and a PIN which can be received on paper. Merchants need to have access to a smartphone or a computer to process purchase transactions.

Summary features

E-transfer mechanism	Beneficiary equipment	Infrastructure at the transaction point	Application
E-voucher	Voucher number + PIN	Merchant with smartphone or computer	Goods/services

*Example from the field***BOX 7: MERCY CORPS E-VOUCHERS WITH VOUCHERPRO BY TRANSVERSAL (NEPAL)**

In early 2013, **Mercy Corps** conducted a pilot in Nepal to provide assistance to some of Kathmandu's poorest residents and test digital vouchers that do not require negotiations with local MNOs or financial institutions. The objective was to identify quality voucher solutions that can be set up quickly, in any location with basic mobile network connectivity.

Mercy Corps partnered the Haitian company, Transversal, to test e-vouchers using a smartphone.

The e-vouchers required the merchant to have a smartphone loaded with Transversal's "VoucherPRO" application and access to a data connection. Beneficiaries did not need to have access to a phone. Instead, they received their voucher number and PIN on paper cards provided by Mercy Corps. To complete a transaction, a beneficiary had to provide his/her unique voucher number and then enter his/her PIN on the merchant's smartphone.

By the end of the pilot, 228 vouchers (100%) had been successfully redeemed. To facilitate merchant reimbursement, VoucherPRO provided reports listing each transaction performed by a merchant and total reimbursement amounts, which were reviewed and approved by programme and financial staff, as well as the merchants themselves. Once all parties confirmed repayment amounts, Mercy Corps wired the amount to the merchant's bank account within a week.

Mercy Corps also tested Transversal's mobile voucher application MerchantPRO using SMS confirmation. While mobile vouchers presented higher error rates and were more difficult for illiterate users to redeem, the e-vouchers were reliable and efficient and are highly recommended for future deployments (where that technology exists). Compared to paper vouchers, both e-vouchers and mobile vouchers offered significant time savings in the merchant reimbursement process and provided access to more detailed data on voucher redemption patterns by beneficiaries.

Source: Murray, S. (2013) *MasterCard Worldwide & Mercy Corps: ELEVATE Phase I Report*. Mercy Corps.

4. BENEFITS AND DRAWBACKS OF E-TRANSFER SYSTEMS

Each e-transfer mechanism comes with benefits and drawbacks. The initial assessment the aid agency conducts to determine if cash is the best option for the intervention will also highlight which potential drawback(s) of an e-transfer mechanism could jeopardise programme success or indeed whether e-transfers are appropriate at all. Above all else, the realisation of programme objectives should dictate which e-transfer mechanism, if any, should be used. In this respect, the importance of the context cannot be overstated.

Which e-transfer mechanism for which intervention?

There is no hard rule that dictates that one mechanism is better suited to one type of programme. Key considerations should centre on the type of restrictions the aid agency may want to attach to the e-transfer, the ease of implementation of a particular delivery mechanism, its cost-effectiveness, the overall benefits to intended beneficiaries including protection aspects, and other imperatives. Table 1, below, recaps the features of the all the e-transfer mechanisms introduced in this section.

Table 1: Summary features of e-transfer services

E-transfer mechanism		Beneficiary equipment	Infrastructure at the transaction point	Application
Cards	Magnetic stripe card	Card + signature (+ PIN at ATMs)	Merchant with PoS or ATM	Goods/services + cash
	Smart card	Card + PIN, signature or biometrics	Merchant with PoS or ATM	Goods/services + cash
	Contactless card	Card + PIN, signature or biometrics	Merchant with NFC PoS or ATM	Goods/services + cash
Mobile transfers	Mobile token	SIM + PIN	Agent with basic phone	Cash
	Mobile voucher	SIM* + Voucher number + PIN	Merchant with basic phone	Goods/services
	Mobile money	Phone +SIM + PIN	Agent/merchant with basic phone	Goods/services + cash
E-vouchers	E-vouchers	Voucher number + PIN	Merchant with smartphone or computer	Goods/services

* not always required

Benefits and drawbacks

Table 2 below provides a non-exhaustive list of benefits and drawbacks for the seven e-transfer options presented.

Table 2: Benefits and drawbacks of e-transfer mechanisms

Transfer mechanisms	Benefits	Drawbacks
Cards		
Magnetic stripe cards	<ul style="list-style-type: none"> - No need for formal ID - No need for a bank account - Relatively low set-up costs - Can be used for cash or commodities - Can be pre-stocked 	<ul style="list-style-type: none"> - Require connectivity and compatible PoS - Proprietary systems restrict number of outlets where the cards can be used - Literacy may be a barrier which poses too great a challenge if the beneficiary cannot read the instructions on an ATM (see Box 12, in section B-3) - Beneficiaries may be charged commission for transactions and withdrawals
Smart cards	<ul style="list-style-type: none"> - Not always need for formal ID - No need for a bank account - Can be used off-line anywhere with PoS - Can be used for cash or commodities - PIN/biometric security protects the cash from theft - Change can be saved on the card 	<ul style="list-style-type: none"> - May require bank account and formal ID - Proprietary systems restrict number of outlets - Could face long set up times for new systems - Literacy may be a barrier which may pose too great a challenge if the beneficiary cannot read the instructions on an ATM (see Box 12, in section B-3) - Beneficiaries may be charged commission for transactions and withdrawals
Contactless cards	<ul style="list-style-type: none"> - Not always need for formal ID - No need for a bank account - Very easy for beneficiary to use - Can be used off-line anywhere with PoS - Can be used for cash or commodities - Change can be saved on the card - Fast to roll out 	<ul style="list-style-type: none"> - Requires formal ID in replacement of PIN - Proprietary systems restrict number of outlets where the cards can be used - High risk of loss of funds if card is lost, since the user doesn't always need to present ID or enter security info to use the card for value up to a particular threshold - Literacy may be a barrier which may pose too great a challenge if the beneficiary cannot read the instructions on an ATM (see Box 12, in section B-3)

Transfer mechanisms	Benefits	Drawbacks
Mobile		
Mobile tokens	<ul style="list-style-type: none"> - Unique authentication code for each transfer increases security - Real time transfer - Fast and discreet - Relatively low set-up costs if handsets are shared - Transactions on the mobile device are done by the agent - Phones can be used for communications 	<ul style="list-style-type: none"> - Formal ID may be required depending on regulation - Network issues may cause delays - Limited by agent coverage and cash flow (liquidity management) - All funds must be withdrawn at once
Mobile vouchers	<ul style="list-style-type: none"> - No need for formal ID - Not limited by agent cash-flow - Reduced risk of theft or fraud compared to paper vouchers - Low hardware requirements - Phones can be used for communications 	<ul style="list-style-type: none"> - Network issues may cause delays - Literacy may be a barrier - Significant training may be required
Mobile money	<ul style="list-style-type: none"> - Fast and discreet - PIN security connected to individual SIM - Relatively low set-up costs if handsets are not provided or are shared - Phones can be used for communications - In some countries, a full suite of transactional options are available which reduces the need to “cash out” (e.g. person-to person transfer, bill payment, etc.) 	<ul style="list-style-type: none"> - Formal ID may be required - Literacy/education may be a barrier and require significant investment in training for new users - Limited by network connectivity - Limited by agent coverage and cash flow (liquidity management) - Cost of providing phones and charging equipment can make set up costs significant - Beneficiaries may be charged commission for transactions and withdrawals
E-vouchers		
E-vouchers	<ul style="list-style-type: none"> - No need for formal ID - Not limited by agent cash-flow - Can be used with any mobile operator - Reduced risk of theft or fraud compared to paper vouchers - Relatively easy for beneficiaries to use - Unspent funds can be saved on the system - Very low hardware requirements 	<ul style="list-style-type: none"> - May require customisation from a provider’s existing platform - Network issues may cause delays - Literacy may be a barrier

Adapted from CaLP (undated) *E-payments in CTP*. CaLP

5. IN-HOUSE/CUSTOM-MADE TECHNOLOGY

Increasingly, aid agencies have considered partnering service providers to jointly design payment scenarios that meet the needs of vulnerable groups, outside of what is already readily available on the market.

The decision to develop one's own customised system should not be taken lightly, however. This option requires strong expertise in e-payment systems, time and may be costly compared to existing commercial options. Some agencies (for instance Mercy Corps in Haiti in 2010 ⁷) have successfully partnered service providers in the midst of launching their new technology solution, as a result developing a service better suited to the needs of vulnerable groups.

The benefits of developing one's own e-transfer system lie in providing the aid agency with a tailor-made service that takes into consideration all the specifics of the programme, including beneficiary capacity, programme design and implementation imperatives, etc.

Example from the field

BOX 8: WFP SCOPE DIGITAL PLATFORM FOR CASH AND VOUCHERS (GLOBAL)



SCOpe (**S**ystem for **C**ash **O**perations) is the **World Food Programme's** (WFP) digital platform for cash and vouchers, leveraging leading-edge technology to deliver humanitarian assistance at scale.

The SCOpe Solutions Suite

1. **SCOpeID:** Electronic beneficiary registration – works “off-line” and can optionally also capture beneficiaries' pictures and fingerprints. SCOpe can also import beneficiary data from other databases, e.g. national safety nets or WFP's cooperating partners.
2. **SCOpeBenefit:** A web-based beneficiary and transfer management solution that allows users to plan, execute and track cash and/or voucher distributions to registered beneficiaries.
3. **SCOpeLink:** Electronic cash/voucher delivery mechanisms that interface with SCOpeBenefit to verify beneficiaries' ID, access beneficiary balances and carry out transactions using those balances. SCOpe is built to use both WFP-designed delivery mechanisms as well as “plug in” to locally available solutions.

⁷<http://www.mercycorps.org/press-room/releases/trilogy-unibank-mercy-corps-team-effort-launch-mobile-money-haiti>

BOX 8: (continued)



1

SCOpeIDbeneficiary registration
(incl. biometrics)**Register and enrol beneficiaries***

*using SCOpe's registration solution or importing from existing databases, e.g. national safety net registries

2

SCOpeBenefit

beneficiary and transfer management

**Plan cash/voucher distributions**

3

SCOpeLink

WFP and external delivery mechanisms

**CASH**

Send distribution instructions to financial service provider

VOUCHER

Generate/top up eVouchers, capture redemption details, update balances

SCOpe relies on a completely open-source technology

Open architecture

SCOpe is ready to integrate with a variety of other databases and applications, including existing safety net, government or partners' identity sources. The core platform (beneficiary and transfer management) is "cloud-based", can be accessed through a web browser on any computer, runs well on slow internet connections.

Open source

The intellectual property for both the core application and the electronic voucher component is fully owned by WFP. The platform leverages open-source technology where possible; this allows WFP to make the platform available to governments and partners at minimum cost.

Open service

WFP is designing a service offering around SCOpe that will offer a range of services to help both WFP country offices and external partners develop their digital transfer capability via SCOpe and adapt it to their needs and unique transfer requirements.

Deployment of the SCOpe system will follow a phase approach in selected countries beginning mid to end 2013.

Source: WFP (2013) SCOpe. System for Cash Operations. The World Food Programme's digital platform to deliver food assistance via cash and vouchers at scale

6. E-TRANSFER ECOSYSTEMS

The minimum requirements

The e-transfers systems used by aid agencies for humanitarian assistance all function in a fairly similar fashion, involving roughly the same type of actors, technologies and devices. The minimum requirements for e-transfer systems to function are listed in Table 3.

Table 3: Minimum requirements for e-transfer systems

Minimum requirements for e-transfer systems
<ul style="list-style-type: none"> • Technology software (platform) and additional hardware in the form of an e-transfer device (SIM card, plastic card, e-voucher, etc.) • Account/e-wallet software (from which the transferred value can be accessed) • Mobile network or internet connectivity (which need not be constant as some systems allow transactions to be conducted off-line) • More than one user with an authorised account/e-wallet (e.g. sender and receiver)

The flow of funds

Mobile- and card-based systems

Here, the aid agency generally converts cash into e-money (digital currency), via bank transfer into the disbursement account created at the e-transfer service provider. There is a constant one-to-one exchange value between the “hard cash” and the e-money in the system. From this disbursement account, often accessible online, the aid agency can transfer cash to its beneficiaries so that they can conduct a variety of e-transactions such as withdrawal, purchases, transfers, bill payment etc., depending on how comprehensive the service is. Some card systems do not require the use of a disbursement account, and bulk payments to beneficiaries can be made directly from the aid agency’s bank account to the beneficiaries’ cards.

The e-money typically resides on either a SIM card in the phone, the chip or the magnetic stripe on a plastic card. The transactions themselves take place at an ATM or an authorised agent/merchant equipped with a PoS terminal or mobile handset. Every time a transaction is conducted, a settlement occurs between two independent accounts – that of the beneficiary and that of the merchant or the ATM.

It is important to distinguish these types of transactions from “online banking”, which refers to a set of authorised transactions (balance check, bill payment, money transfer) that only existing bank account holders can initiate over the internet (via a personal computer or a smartphone) and notably does not allow users to withdraw cash or make purchases at retail locations.

E-voucher systems

Here, merchants can be reimbursed after the sale of goods and there is therefore no direct e-commerce transaction at the point of sale. Rather, the funds are held by the aid agency and transferred to the merchant directly on an agreed timeframe, after authentication of the e-voucher following beneficiary purchase and verification of the related e-voucher redemption reports.

Authentication

The most widely used method to authenticate a transaction requires a PIN. Other authentication methods can include signatures or biometrics (finger prints, iris scan, etc.). Attention must be drawn to the fact that, the use of biometrics may, in some contexts, offer new opportunities for undocumented beneficiaries to access aid. In others, issues can be experienced such as cultural resistance to providing biometric data and limited transferability of their entitlement to a trusted family member or friend for housebound beneficiaries, when the biometric data of this other person are not recorded on the system.

In some countries, depending on legislation, a government-issued ID is also required when redeeming an e-transfer for cash.

The web of actors

Private sector partners are essential in the delivery of e-transfer services. As shown in Table 4 below, these services may be offered by a wide range of providers.

Table 4: Range of e-transfer service providers

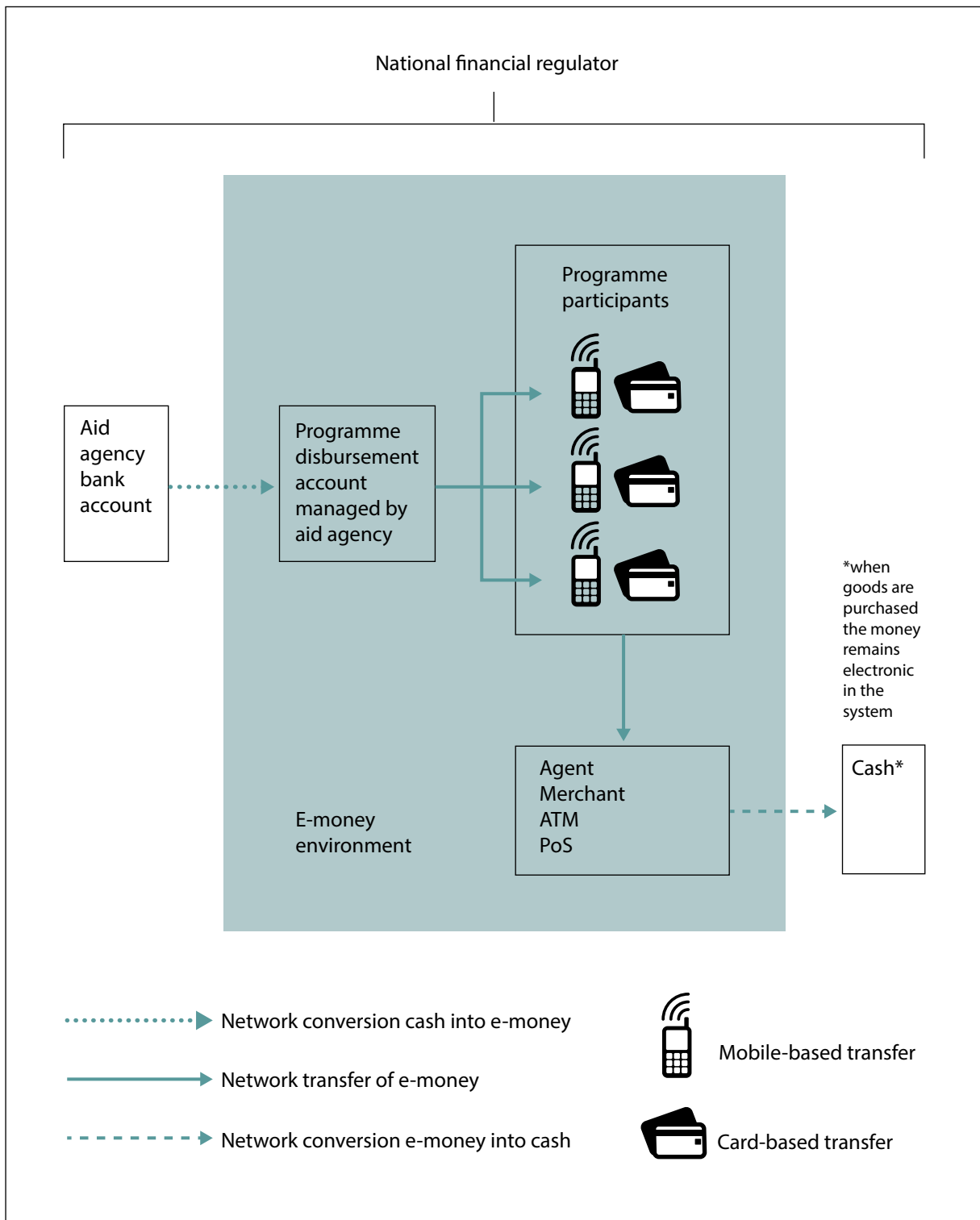
E-transfer services providers can be...
<ul style="list-style-type: none"> • a mobile network operator (MNO) • a bank or another form of financial institution • an authorised third party (e.g. a payment company such as Visa and MasterCard) with or without a bank partnership • an aid agency using a third party payment platform • any combination of the above

These providers are part of the many actors that form an e-transfer ecosystem. They perform the following functions:

- **The national financial regulator**, usually the central bank, issues the regulation governing e-transfers including customer due diligence requirements which stipulates the type of identification documents senders and receivers of e-transfers must provide, sets limits on transaction amounts and volumes, determines reporting requirements, etc.
- **The banks/financial institutions** maintain an account of the funds available in the system. In card-based transfers, they will also issue the card. They may also provide PoS devices to merchants and ATM facilities for cardholders to connect to the network. In mobile transfers, they may assume responsibility for the agents depending on the regulation.
- **The network operator** provides the payment-processing infrastructure, connecting all other actors in the process.
- **The merchants** accept digital forms of payment (mobile money, mobile vouchers or e-vouchers) for the goods they sell.
- **The agents** support customers to convert e-money into cash and cash into e-money. It is not uncommon for agents to also act as merchants.
- **The users (programme participants)** exchange e-money received from an aid agency via e-transfer for cash, goods or services.

Figure 1, below, provides an illustration of the flow of funds in an e-transfer ecosystem combining both mobile- and card-based transfer options in the context of a humanitarian assistance programme, and presents these key actors at play.

Figure 1: Illustrative humanitarian e-transfer ecosystem





SECTION B: CHOOSING E-TRANSFER MECHANISMS



PHOTO: SURAJ SHAKYA

The choice of what e-transfer mechanism to use for a given programme must not only be considered in light of the choice of mechanisms available but also in light of the context of the intervention and the strategy of the aid agency.

This section is concerned with helping agencies make the decision as to which e-transfer mechanism(s) may be most appropriate for their intended programme, considering a range of factors and conditions such as **preparedness measures, cost analysis, beneficiary preferences, private sectors partnerships** and **regulatory concerns**.

KEY LEARNING POINTS



- The main service providers for e-transfers are banks, MNOs, third party license providers and aid agencies themselves (when they directly licence out a technology).
- Engaging private sector partners for e-transfers can be a lengthy process which aid agencies are best to begin ahead of an emergency, as part of a preparedness plan.
- Potential service providers should be evaluated based on key assessment criteria and commitment to a minimum level of service.
- Adopting a partnership approach with e-transfer service providers and building operational collaboration positively influence programme quality.
- Aid agencies should inquire about the financial regulations applicable in the country of operation to anticipate the identification requirements for beneficiaries and transfer conditions (number of transactions allowed, scale and volume).
- Collaboration and coordination with other aid agencies with experience in e-transfers in the area of operation can help agencies better design their own intervention, through sharing of best practice, as well as negotiate better terms and conditions with service providers, individually or as part of a consortium.

I. GETTING STARTED WITH E-TRANSFERS

The e-transfer planning process

Before any e-transfer can be made, an aid agency is typically required to undertake the steps described in Table 5, below, with approximate time estimations and bearing in mind that some of the steps identified can be carried out simultaneously by different teams. These estimates assume that the agency has already taken a decision to deliver a cash transfer programme and has completed all the necessary design work, including identification of the beneficiaries, calculating the value and frequency of the benefit.

How long each of the steps will take depends on such elements as:

- the context and size of the intervention;
- the level of maturity of the market and the range of options available;
- the proactiveness of the service provider and the aid agency in contract negotiation;
- whether unforeseen events/obstacles occur.

Table 5: E-Transfer planning process

E-Transfer planning process	Estimated time
1. Assess the commercial landscape of services and providers	2 weeks
2. Understand the regulatory context surrounding the e-transfer options under consideration	
3. Negotiate and sign a service contract with the chosen service provider (including tendering process and contract vetting by aid agency legal teams at HQ)	3-6 weeks
4. Ensure compliance of the e-transfer service with internal and donor requirements	1 day
5. Open an account at the partner bank of the service provider – optional	3 working days
6. Order e-transfer devices (cards/SIMs/mobile vouchers, e-voucher batches, etc.)	1 week or more
7. Register beneficiaries with associated e-transfer devices and train them on how to use the e-transfer device <i>In the case of a voucher programme, register and train merchants</i>	Depends on the size of the beneficiary (and merchant) population
8. Set up a disbursement account from which e-transfers to beneficiaries will be made – optional	1 week
9. Receive training on using the online interface to access the disbursement account	2 days
10. Populate beneficiary data and make a transfer	1 day
Total	> 2.5 months

Ecosystem considerations such as the number of agents/ATMs/PoS devices are relevant as a ratio and spread of a sample beneficiary population. For example, a service that can make available five agents with a high level of liquidity within a 5km radius of the beneficiary community may prove more useful to a programme than 50 agents 50km away with moderate liquidity.

In more mature markets, service providers have stronger processes in place, which they can adapt more easily and faster to an aid agency's needs.

Conversation with the service provider will shed light on these aspects, which will help the aid agency make an informed decision on what service to choose.

The commercial environment***The service providers – who to turn to for what?***

When considering e-transfers, gaining a good understanding of the major actors in the area of intervention is key.

An assessment of the commercial environment of e-transfer services and providers should be included as part of a preparedness plan to identify a number of different providers with the capacity to deploy a service in the anticipated area of intervention and possibly negotiate preferred supplier agreements, ahead of an emergency.

Whilst Figure 1, in [Section A-6](#), provides an illustration of the flow of funds in an e-transfer ecosystem and its main players in the context of a humanitarian assistance programme, Table 6, below, presents the various providers and the e-transfer services they generally offer.

Table 6: Service providers and their associated services

Provider	Service	Cited example
Bank	<ul style="list-style-type: none"> • Cards and card systems • ATMs/PoS • Mobile money accounts 	Philippines Veterans Bank (the Philippines, Box 1), Cairo Amman Bank (Jordan, Box 2)
Mobile Network Operator (MNO)	<ul style="list-style-type: none"> • Mobile network connectivity and data • Mobile wallets • Mobile-based transfers 	Safaricom (Kenya, Box 17), Airtel (Niger, Box 6)
(Non-bank) Financial Institution	<ul style="list-style-type: none"> • Cards and card systems • Payment services for e-vouchers 	Wari (West Africa, Box 4), sQuid (Kenya, Box 3),
Third party software developers/platform vendor	<ul style="list-style-type: none"> • E-voucher software • Payment platforms 	Transversal (Nepal, Box 7 ; Haiti, Box 5)

Additional guidance

This commercial assessment should be done with support from the procurement team and in accordance with internal/donor processes.

A review of the procurement process for an e-transfer service provider is presented in [Section E-2](#).

What service to expect

During this commercial assessment process, aid agencies must ensure that service providers can guarantee a minimum level of service, as described in Table 7, below.

Table 7: Minimum level of service for e-transfer service providers

Minimum level of service for e-transfer service providers
<ul style="list-style-type: none"> • Adequate connectivity to support e-transfer transactions • Acceptable transaction limits on the e-transfer device (number and value of the transactions that can be carried a day/a month suited to the needs of the targeted beneficiaries) • Sufficient presence of cash collection/transaction points • Acceptable maximum travel distance to cash collection/transaction points • Adequate levels of liquidity (cash availability at agent) • Technical support (technical issues, PIN number reset, use of the disbursement interface, error correction, etc.) • Reporting processes that meet agency and donor requirements • Willingness to sign aid agency's code of conduct including for data protection • Acceptable risk management procedures (particularly regarding privacy and security)

Additional guidance

A list of criteria to consider when selecting an e-transfer service provider is presented in [Section E-3](#).



PHOTO: CAROLINE BERGER/OXFAM

2. ASSESSMENT CHECKS FOR E-TRANSFERS

Key elements to consider

What the best transfer mechanism is for a given programme should be determined by considering a number of parameters as described in Table 8, below. This assessment will allow the aid agency to contextualise the use of a given e-transfer mechanism to the intervention objective, resources, scale, and quality standards.

Table 8: Assessment criteria of e-transfer mechanisms

Criteria	Description
Programme objective	Positive change desired from the intervention including whether wider benefits are sought through access to technology
Cost	Cost of the different options to both the aid agency and the recipient (including not only the cost of the transaction but also all the costs of designing, implementing and monitoring the programme)
Security	Level of physical safety for staff and recipients
Control/risks	Systems that are needed to manage risks such as fraud and error as well as beneficiary data protection. Consider the level of automation, security in the system and at the cash collection and transaction points, the ability to monitor and rapidly make corrections, and security in the reporting and reconciliation process
Human resources	Number of staff required and their level of skills, education, ability to provide training to recipients, etc.
Speed	Time taken to roll out the solution
Acceptability to vulnerable groups	Comfort with use as expressed by recipient and “on the ground” providers, need for support, convenience
Resilience	Ability to recover data and to continue the service when the environment is difficult or changes suddenly
Scale	Effectiveness of the different options at operating on a large scale
Flexibility	Ease with which the chosen option can be adjusted to vary payment amounts and other changes
Registration requirements	Type of identification required for beneficiaries to subscribe to e-transfer services
Compliance requirements	Ability of the system to meet both internal and donor requirements for reporting

Adapted from Harvey, P., Haver, K., Hoffman, J., Murphy, B. (2010) *Delivering Money. Cash Transfer Mechanisms in Emergencies*. CaLP

Focus on cost

Of all the above-mentioned criteria, cost is perhaps the most challenging for aid agencies to assess. Many cost parameters are often difficult to evaluate.

First, there are perceived relatively high set up costs associated with providing e-transfers devices such as SIM cards, handsets (when needed) and payment cards for beneficiaries to participate in the programme. In addition, fees charged by providers can also be difficult to understand relative to the service and support to be expected. Furthermore, depending on the complexity of the intervention, sets-up costs for the aid agency will go beyond providing e-transfer devices and training, to include partaking in activities to improve the e-transfer ecosystem such as recruiting agents or training merchants on using e-transfers, which can be costly.

Thus below are a few examples of how costs can be assessed.

Simple scenario-based approach to understanding costs

Because some costs are fixed and others are variable, it is important to assess costs over the entire duration of the programme to evaluate whether economies of scale are achieved.

Scenario planning is a “quick and dirty” assessment to compare the cost of different e-transfer mechanisms. It is well suited for mature e-transfer systems where cash collection and transaction points are well-resourced and ubiquitous, and the set-up costs associated with each e-transfer mechanism are therefore similar.

Example from the field

BOX 9: OXFAM AMERICA CASH PREPAREDNESS PLAN (SENEGAL)



In February 2013, **Oxfam America** sought to determine the most feasible option(s) for transferring cash at scale in the most timely and efficient manner in future emergencies and to make recommendations for preparedness actions including technical capacity, contingency planning, improved coordination, and internal systems. As a result a cash preparedness plan was produced.

On the specific issue of cost, compiling all fees quoted by e-transfer service providers, three scenarios were envisioned, all based on a transfer of 40,000 FCFA (\$80) to 1,000 beneficiaries and aligned with possible programme durations:

- Scenario 1 assumes one transfer (one month)
- Scenario 2 assumes three transfers (three months – past programmes)
- Scenario 3 assumes five transfers (length of the lean season)

This approach was used as none of the options required ecosystem interventions from Oxfam.

Service	Quoted fee	Transfer fee	Cash out fee	Cost of card	Scenario 1 (1 month)	Scenario 2 (3 months)	Scenario 3 (5 months)
EcoBank salary card (min)	Transfer fee: 300 - 500 Card: 6,000 -10,000	300	0	6,000	46,300,000	126,900,000	207,500,000
EcoBank salary card (max)		500	0	10,000	50,500,000	131,500,000	212,500,000
MoneaCard (Ferlo GIM-UEMOA)	Cash out fee: 500 Card: 2,500	0	500	2,500	43,000,000	124,000,000	205,000,000
Orange Money	Cash out fee: 1-10,000 CFA = 6% Transfer fee: 1-10,000 CFA = 100 CFA	10%	6%	0	46,400,000	139,200,000	232,000,000
WARI (Min)	1,200 - 1,400 per transfer	1,200	0	0	41,200,000	123,600,000	206,000,000
WARI (Max)		1,400	0	0	41,400,000	124,200,000	207,000,000

Adapted from Sossouvi, K. (2013) *Cash Preparedness in Senegal – Cash Transfer Mechanisms*. Oxfam America

CaLP cost-effectiveness research methodology

A comprehensive analysis of programme costs can be conducted to determine the overall programme budget. To determine the likely costs associated with a particular programme design, it is useful to know not only what the funds will be spent on – salaries, fuel, printing, etc. – but also how these items will be used, such as registering beneficiaries, disbursing the transfer or post-distribution monitoring. This enables programme managers to consider whether any activities can be made more efficient. This approach allows the aid agency to consider costs relative to the activities to be conducted as opposed to comparing the cost of different options between themselves.

Example from the field**BOX 10: CALP COST-EFFECTIVENESS RESEARCH (GLOBAL)**

As part of the research on the Factors Affecting the *Cost-efficiency of Electronic Transfers* (2013) in Humanitarian Programmes commissioned by CaLP, the Oxford Policy Management Group (OPM) designed a comprehensive cost-effectiveness assessment methodology.

A matrix of costs can be set out in a spread sheet with the two axes as follows:

Costs by line item. List items of expenditure in the first column. These will include personnel costs, transport and travel, printing, communication and other general office overheads, commission to payment providers and management fees.

Costs by activity. List activities in the first row. This will include programme design, institutional arrangements (such as contract negotiation), advocacy, training, targeting, disbursement, and monitoring and evaluation.

When the matrix has been completed with the estimated costs required to run the programme over a defined time period, the activities can be split into those that occur once only, such as the programme design or an endline impact evaluation, and those that happen with every payment, such as the cost of overseeing the disbursement of cash and maintaining a helpline for queries and complaints. The estimates can then be varied to see how the number of transfers affects the total cost: the one-off activities will remain at a fixed cost, provided that the programme design does not change, while the recurrent costs will vary.

A series of case studies in Kenya and Somalia have been done using this matrix and are presented in the report on the cost-effectiveness of electronic transfers that accompanies these guidelines.

Source: O'Brien, C. Hove, F. and Smith, G. *Cost-effectiveness of e-transfers*. A report commissioned by CaLP and due for publication in Dec 2013.

NetHope⁸ costing tool

Aid agencies transitioning from manual cash transfers to e-transfers may be interested in documenting their choice by comparing the costs of the two programme options.

Example from the field

BOX 11: NETHOPE COSTING TOOL (GLOBAL)



A comprehensive cost assessment tool was developed by NetHope to provide an analytical framework for organisations to compare the identified costs of cash with the costs of transitioning and using e-payments in the long term.

The tool is an Excel workbook designed as a guide for organisations to conduct a comparative evaluation of the non-financial and financial costs of using physical cash and e-payments, in their programming and administration. It suggests categories of costs that organisations may incur in using cash and e-transfers. These categories can be expanded and modified to fit the programme profile.

The tool is available for download at <http://cloudportal.nethope.org/programs/payment-innovation>

Source: NetHope

⁸ As part of Global Broadband and Innovations (partnership with USAID), NetHope promotes the use of technology in humanitarian interventions, and actively seeks to help their partners make the transition to e-payments by providing grants, tips, processes and tools: <http://nethope.org/>

3. PREPAREDNESS AND CONTINGENCY PLANNING

Engaging private sector partners for e-transfers can be a lengthy process which aid agencies are best to begin ahead of an emergency and, where possible, collectively. Poor consideration of the time or the actions necessary for the appropriate set up of e-transfers can lead to challenges down the line, which can delay programme implementation.

Key elements to consider

Risk assessment: An emergency risk assessment can be conducted to determine whether e-transfers are a viable option in a pre-emergency context, by answering questions related to the appropriateness of the intervention, its feasibility from a logistical, time and cost effectiveness perspective, whether it meets finance requirements in terms of speed and accountability as well as security measures for aid agency staff and beneficiaries (see [Section E-4](#)).

Building the ecosystem: To meet the requirements of a humanitarian intervention, depending on the level of maturity and scale of their systems, service providers may need to increase cell signal; enrol and train additional agents; set up temporary ATMs; recruit and train temporary staff, etc. In some instance, changes to the actual system to add new functionalities, meet the reporting needs of the aid agency or other demands, may also be necessary. All these activities will require considerable time to implement as well as a cost-benefit analysis by the service provider and will involve decision-making in consultation with senior executives.

Preparation and pre-positioning: Some aid agencies aspire to include in their preparedness plan to pre-register beneficiaries living in disaster prone areas in anticipation of providing future assistance.⁹ During this process, introducing beneficiaries to e-transfer methodologies could also be considered. This brings the benefit that, in the event of a sudden-onset emergency, aid agencies will not have to resort to the delivery mechanism which they can scale-up rapidly, but the one which is the most adapted and cost-efficient. Finally, depending on costs and feasibility, pre-positioning e-transfer hardware (SIMs, cards, etc.) with service providers can also be considered.

Contracts: Sufficient time must be allowed for the review of contracts and signature process on both sides – service provider and aid agency – as contracts may require the involvement of senior managers or legal teams in headquarters who are not always readily available.

Consultation: Great value can be derived from researching what government disaster plans intend to use e-transfers. This will not only ensure that the proposed humanitarian intervention is coherent with national priorities but will also help aid agencies negotiate better deals with service providers. This is also true for collaboration and coordination with other aid agencies with experience in e-transfers in the area of operation. This can help agencies integrate lessons learned and thus better design their own intervention as well as, again, negotiate better terms and conditions with service providers, individually or as part of a consortium.

Collaboration to reduce costs: Where agencies are likely to use the same e-transfer partner, collaboration is necessary to better understand the capacity of the service provider to meet the beneficiary caseload, locations and frequencies, etc. In addition, a collective caseload may be more attractive to the service provider and thus additional services (such as improving coverage, providing additional staff) or reduced costs/charges may be possible.

Piloting: Preparedness measures can also include running small-scale pilots to build understanding of e-transfers and capacity at implementing them in future emergencies. Aid agencies staff need to be aware of a number of operational aspects required in implementing e-transfers. Piloting a response can be a good methodology for building capacity and confidence in using new transfer mechanisms. In addition, piloting allows senior management an insight into their team's capacity (and training needs) as well as the feasibility of using the modality in an emergency.

⁹ Austin, L. and Frize, J. (2011) *Ready or Not? Emergency Cash Transfers*. CaLP. Valid International.

*Example from the field***BOX 12: OXFAM GB CASH GRANTS WITH UBL (PAKISTAN)**

In 2011, as part of its study on innovative payment methods in Pakistan, **Oxfam GB** carried out a pilot-run of United Bank Limited's (UBL) WIZ magstripe prepaid debit card in Upper Sindh. The objective of the pilot was to understand the WIZ card's viability and effectiveness as a payment method in on-going and future cash transfer programmes in the country.

Fourteen beneficiaries of Oxfam's "Community Conditional Cash Grant" activities as part of the flood response were selected. The pilot run was carried out on a small scale without formal arrangements with UBL, which considerably speeded up programme implementation. Cards were bought off-the-shelf to understand the overall process and enable the identification of key issues that would need to be addressed for large-scale usage.

The following steps were required to register on the system:

STEP 1	Fill out the application form, sign and deliver to any online UBL branch along with a copy of the Computerised National Identity Card (CNIC) and initial deposit (minimum PKR 500 per card).
STEP 2	Collect the WIZ card from the branch after 2-3 days and call the help line for activation of the card. The helpline will activate the card after due verification of the caller/applicant. This activation will be subject to confirmation of the CNIC, which usually takes 24 hours.
STEP 3	After the card is activated, a second call is placed to the helpline for PIN generation. After answering a series of verification questions correctly, the applicant is asked to punch in his/her four-digit PIN.
STEP 4	Withdraw cash from any specified ATM.

(continued overleaf)

BOX 12 (continued)

The pilot recorded many challenges and lessons learnt:

- Beneficiaries were not able to fill in the one-page English application form unassisted.
- The bank did not accept thumb impressions and required proper signatures from beneficiaries, who were for the most part illiterate.
- There were problems in getting through to the helpline due to network traffic, including lengthy on-hold times, of up to 20 minutes per cardholder in some cases.
- Beneficiaries were often unable to understand and respond to verification questions asked by the helpline operator despite arranging a local language operator.
- Beneficiaries had no prior ATM experience, an issue that was only secondary to the fact that they could not read the options on the ATM screen.
- Project staff had to facilitate cash withdrawal from the ATM with the beneficiary standing by their side and observing the process.
- Only one of the three females came to the ATM for cash withdrawal, with the other two sending their male relatives.

As a result of these challenges, subsequent payments to the same beneficiaries were done through cheques, which had been the payment method previously used for them, and for other beneficiaries in the programme. This decision was taken after experiencing delays in the receipt and activation of the WIZ cards, and the number of man-hours required by Oxfam and partner staff to support the beneficiaries for registration and withdrawal of cash.

Source: Nawaz, A. (2011) *Pakistan Flood Response: Piloting Cash Transfers through Prepaid Debit Cards*. Oxfam

Additional guidance

A preparedness risk assessment tool is presented in [Section E-4](#).

4. BENEFICIARY PREFERENCES AND PROTECTION

E-transfers can carry a strong novelty factor for their future users. Their use should therefore, as much as possible, be contextualised to the preferences and habits of the targeted beneficiaries.

Aid agencies should seek to identify beneficiaries' perceptions of the various e-transfer mechanisms by asking questions such as: do beneficiaries feel that one transfer mechanism puts them in greater risk than another? Are they concerned about their e-transfer device being stolen? Are illiterate members of the community able to cope with the system or will they be vulnerable to others taking advantage of them? These issues should be identified early as they can often be overcome through training and awareness-building.

Key elements to consider

Past experience and skills: Understanding what e-transfer mechanisms and devices beneficiaries are already familiar with can support the decision of what option to use in a programme.

For example, enquiring about the level of comfort with mobile phones by assessing habits such as balance checking, airtime transfer, etc. can give the agency a good indication of the type of training that will be required, if mobile transfers are to be used. Similarly, past experience with sending and/or receiving remittance is valuable information in choosing a potential service provider and anticipating future challenges. Other key end-user considerations are the level of financial literacy and network preferences (especially in markets where services from different providers are not interoperable).

This will help the aid agency determine whether the majority of the beneficiaries will be able to independently complete a transaction. If not, they will be forced to rely on family or community members and agencies will need to build robust systems to ensure that intended beneficiaries retain control of the transfer process.

Protection and gender: It must also be emphasised that e-transfers can have positive protection impacts for beneficiaries. Through e-transfers, aid agencies have been able to provide financial support directly to women and other vulnerable groups, thus giving them direct control over their money and empowering them to positively impact on the lives of their families.¹⁰

Understanding the vulnerabilities and opportunities associated with protection and gender issues is key to avoid harmful practices and to align e-transfer programmes more closely to the needs of the target population. This includes analysing the distinct challenges women and men face and how those challenges might be impacted by the e-transfer programme.¹¹

Sensitisation: Mobile phones have often been cited as a useful tool for two-way communication and dialogue with beneficiaries, and can be used for sensitisation and accountability to beneficiaries. Having said this, some aid agencies have also reported that, at first, beneficiaries are reluctant to use their programme mobile phone for communication for fear of losing it. Sensitisation on this issue to build confidence and put beneficiaries at ease is important.

¹⁰ USAID (2012) *Standards and Practices Report for Electronic and Mobile Payments*

¹¹ Berg, M. Mattinen, H. and Pattugalan, G. (2013) *Case Studies of the World Food Programme (WFP) and the United Nations High Commissioner for Refugees (UNHRC) Assistance*.

*Example from the field***BOX 13: WFP/ACF UNCONDITIONAL MOBILE TRANSFERS WITH MTN (CÔTE D'IVOIRE)**

Following the post-election violence in Côte d'Ivoire in late 2010, the **World Food Programme (WFP)** selected **Action Contre la Faim (ACF)** as its implementing partner and mobile operator MTN as the financial service provider for mobile transfers to households in two of the most affected municipalities of Abidjan: Yopougon and Abobo.

The “Save Lives and Protect Livelihoods in Emergencies” programme aimed to improve food consumption among vulnerable households by providing the cash equivalent of the value of a monthly basic basket of food rations for two months, through mobile transfers.

While not designed with specific gender-related objectives, the programme targeted women as beneficiaries and set an indicator of achievement at 70%, which was more than met, as approximately 90% of recipients were women. In addition, specific attempts were made to ensure that single parent households were included, including single male parents.

Although targeting a woman for an e-transfer does not necessarily mean that she will make decisions on purchases independently, most female beneficiaries in the programme, however, consistently reported that it was either they alone that decided how to spend the money (73.5%) or that it was a joint decision with their spouse (20.6%). Thus, the evaluation identified considerable empowerment impacts, with women taking confidence from making financial decisions and from the independence created by the income generation opportunities. Women also reported being able to prioritise education for their girls. The discreet nature of the mobile transfers allowed some women to keep their payment secret.

The evaluation was unable to uncover any incidences of favours having to be performed for either inclusion in the programme or for encashment, nor any reported incidence of gender-based violence as a result of the programme in focus group discussions, questionnaire or informal interviews, nor does it seem that intra- or inter-household relations have been substantially affected. The evidence collected and reviewed through the evaluation overwhelmingly suggests that not only did women not become targets/victims of aggression as a result of this programme, but it rather provided a certain degree of empowerment.

Opinion among institutional partners, project staff and beneficiaries themselves was nearly universally supportive of the decision to target women. The reasons given included the recognition that it was women who were primarily responsible for the purchase, preparation and distribution of food within the household, as well as healthcare, and education. It is the opinion of the evaluators that the targeting of women in this case was one of the major successes of the programme, as it was implemented.

Truelove, S. and Wilson, M. (2012) WFP/ACF *Unconditional Mobile Cash Transfer in Abidjan, Ivory Coast. External Evaluation*

Additional guidance

A sample e-transfer usage survey is provided in [Section E-5](#).

5. PARTNERING WITH SERVICE PROVIDERS

Negotiation

Negotiation with e-transfer service providers is often a daunting prospect for aid agencies. In many markets, there may only be one provider offering e-transfer services suited to a particular aid agency programme, which may appear to further reduce bargaining power.

Key elements to consider

Partnership management: Adopting a partnership approach with e-transfer service providers and building operational collaboration positively influence programme quality and can bring effective results in tailoring the service to the needs of the beneficiaries and improving their user experience. The objective of the partnership should be defined clearly internally from a strategic, programme impact and operational ‘perspective’ and communicated with the same clarity to the service provider.

Audience: Conversations should be held not only with sales representatives but also with decision makers with the power to sign off on major commitments.

Language: Aid agencies must adopt a rhetoric and dialogue that matches corporate culture. While the long-term benefits of new subscribers created by the humanitarian programme is of major interest to service providers, it may not always be a compelling argument given the socio-economic makeup of target beneficiaries, often being marginalised, under-represented communities. It may thus be necessary for aid agencies to “translate” their humanitarian message in ways that might be more easily understood and appreciated by a potential service provider. In these discussions, key data and projections are useful to have on hand, such as: transaction volumes, total monetary value of the transfers over the course of the programme, frequency of e-transfers, regional focus of the intervention, etc.

Consultation: Collaboration and coordination with other aid agencies with experience in e-transfers in the area of operation can help agencies integrate lessons learned and thus better design their own intervention as well as to negotiate better terms and conditions with service providers, individually or as part of a consortium.

Alignment: Expectations should also be aligned. With e-transfers, especially when the e-transfer device is new to the beneficiaries, aid agencies act as facilitators for a potentially longer-term commercial relationship between the beneficiaries and the service provider. As mentioned, on one hand, this is a negotiation argument to improve the aid agency’s bargaining position with a service provider. But, on the other, this also activates the fear many agencies may have that, as a result of this relationship, services providers may try to on-sell services to beneficiaries which may not be appropriate or affordable.

*Example from the field***BOX 14: OPENREVOLUTION (US)**

OpenRevolution is a US-based mobile financial services advisory firm. It regularly supports aid agencies to foster partnerships with mobile network operators and financial institutions providing mobile money services. It stresses the importance of using language that is meaningful to service providers.

Humanitarian programme description

“Our programme provides monthly cash stipends to thousands of vulnerable households impacted by the recent floods so they can buy approved food stuffs from authorised traders. The programme will last from January to July and we’re focusing our activities in the centre and south of the country.”

Message to service provider

“We’re going to identify and train up to 10,000 households to receive \$250 a month electronically for seven months to buy food. That’s 70,000 transfers worth \$17.5 million over the lifetime of the programme with at least an additional 70,000 retail purchases. We also intend to identify and train 40-50 merchants to participate in our programme. We’re operating in two of the more densely populated rural districts in the country.”

Source: OpenRevolution

Additional guidance

An interview guide/checklist of key issues with service providers is presented in [Section E6](#).

Service contracts and MoUs

The details of the partnership between the aid agency and the service provider should be articulated in a service contract or a Memorandum of Understanding (MoU). Aid agencies should ensure that contract discussion and signature involves not only their programme and procurement teams but also their finance director and, if necessary, the ICT specialist. **Before signing any type of agreement, aid agencies should insist on live demonstrations of the service and online interface.**

In addition, specific attention should be paid to the elements presented in Table 9 below.

Table 9: Key elements of an e-transfer service contract

Topic	Description
Pricing	<ul style="list-style-type: none"> • All fees charged to the aid agency for making a transfer and to the beneficiary for withdrawing cash and/or making payments. • Additional fees charged for daily operations such as balance check, access to customer service, etc • Whether or not the system can be configured so that all fees incurred can be covered by the aid agency so that beneficiaries receive the net value of their entitlement • Costs for any changes to the system to customise it for programme context or to meet donor reporting requirements, etc. (if they are to be borne by the aid agency)
Hardware, equipment and cash delivery infrastructure	<ul style="list-style-type: none"> • Cost and conditions of procuring SIM cards, phones, cards and making available PoS terminals and/or ATMs • Presence and number of cash collection and transaction points • Distance to travel to access cash collection and transaction points • Opening hours/daily availability of cash collection and transaction points
Online interface	<ul style="list-style-type: none"> • Conditions of use of the online interface from which to manage transfers • How transfers are initiated and by whom (aid agency or service provider) • Control mechanisms (viewer/maker/checker rights)
System security and data integrity	<ul style="list-style-type: none"> • Security protocols of the system including measures to mitigate against and identify responsibility in the case of fraud • Traceability of funds in real time • Resilience to foreseeable hazards, prolonged shut-downs, etc • Processes whereby transactions can be recalled in case of errors • Specific data protection clauses which address the privacy-related risks of e-transfers • Up-time report, showing how often the network is down (if dealing with an MNO)
Technical support to aid agency	<ul style="list-style-type: none"> • Level of technical support the aid agency is entitled to expect with the online interface and in the field working with merchants and agents, including maximum delay for troubleshooting by the service provider • Training and support to the beneficiaries in using the e-transfer mechanism and collecting their e-transfer • Ability of the service provider to dedicate a corporate call centre account, in order to ensure the aid agency receives support above that of an everyday customer
Reporting	<ul style="list-style-type: none"> • Reporting functions that meet donor and internal requirements • Clarity on who can generate reports (aid agency, service provider, or both)
Roles and responsibilities	<ul style="list-style-type: none"> • Roles and responsibilities of each party with strict termination clauses

Additional guidance

Additional minimum contract requirements are provided in [Section E7](#)

6. CASH TRANSFER REGULATORY ISSUES AND BENEFICIARY REGISTRATION

Money transfers can create risks of money laundering and terrorism financing when senders and receivers are not properly identified and vetted. Mitigation against these concerns is managed by the central bank and national regulators of each individual country in the form of anti-money laundering and counter-financial terrorism (AML/CFT) regulations. Depending on the country, senders and receivers of fund transfers may be required to provide varying levels of identification to complete the customer due diligence process through Know-Your-Customer (KYC) procedures.

Key elements to consider

Typically, the basic type of information needed to meet KYC requirements are:

- name;
- date of birth;
- address;
- telephone number;
- proof of identify (typically National ID card or another valid formal identification such as birth certificate, driver's license, or passport).

Applicable legislation: It is useful to inquire about the financial regulations applicable in the country of operation, including AML/CFT rules, to anticipate the documentation beneficiaries may be required to provide and transfer conditions (number of transactions allowed, scale and volume). In the absence of this information, aid agencies may have to rely on service-provider requirements which may not always represent the best reading of the regulations as it pertains to humanitarian cash transfers.

Financial inclusion: Generally, financial institutions must adhere to stricter KYC procedures than MNOs given their role in the domestic economy. Therefore, they may adopt a more conservative policy vis-à-vis KYC when providing e-transfer services versus an MNO. However, in some countries, the central bank can request that MNOs follow a “bank-led model”, which requires them to apply the same strict KYC policies as banks. Having said this, many regulators have made efforts to balance the objectives of AML/CFT with increasing financial inclusion, which opens the door for negotiating a reduced beneficiary KYC regime.

Fiduciary checks: In many countries, aid agencies are required to check that the service providers they are considering signing a contract with do not appear on international lists of excluded parties. Such a fiduciary check may also be a donor requirement due, for instance, to counter-terrorism legislation in donor countries. In some countries, these checks also need to be applied to beneficiaries. Knowledge of the legal requirements of both donor and recipient countries is therefore key.

Data protection: It is important the aid agency reminds the service provider of its data protection policy and defines clear processes regarding the disclosure of beneficiary KYC information for the duration of the programme and after the beneficiary stops using the service. Sometimes, the technology itself may dictate the KYC requirements. For instance, in many closed loop systems, as long as the sender of funds is well identified, recipients need not be.

*Example from the field***BOX 15: BANQUE DE LA RÉPUBLIQUE D'HAÏTI
KYC REQUIREMENTS (HAITI)**

The launch of mobile money in Haiti following the devastating 10 January 2010 earthquake occurred in a context of limited regulation governing electronic transfers. Yet the Banque de la République d'Haïti (BRH), Haiti's Central Bank, reacted with flexibility by allowing tiered KYC requirements.

Mobile money users are allowed to subscribe to a "mini mobile wallet" automatically by keying a short code on their phone. The mini wallet stores up to 4,000 HTG (\$100) at any one time. No additional KYC is required to activate this account beyond the information provided by users when they first acquire a SIM card, namely a photo ID and an address.

Subscribers willing to store a higher value can request a "full wallet" capped at 10,000 HTG (\$250) by filling out a form at an authorised retail location (bank branch, MNO outlet, or agent) and providing a government-approved ID and address.

Thanks to this regulation, many NGOs were able to launch e-transfer programmes using the mini-wallet. Out of the 14 e-transfer programmes implemented worldwide in 2011, six were in Haiti, using the mini wallet.

Source: Sossouvi, K. (2012) "Innovation in Emergencies: The Launch of Mobile Money in Haiti" in Humanitarian Exchange Magazine, *Special Feature: New Learning in Cash Transfer Programming*. Issue 54, May, pp.18-20 and Dalberg (2012) *Plugging into Mobile Money Platforms*. Early Experiences of NGOs in the Field



PHOTO: JANE BEESLEY/OXFAM

SECTION C: USING E-TRANSFER MECHANISMS



PHOTO: SURAJ SHAKYA

This section illustrates the process of setting up and using e-transfer mechanisms by reviewing the **implementation skills** required, the systems used as well as **measures to increase participation of the most vulnerable groups, and how to mitigate against fraud and errors and ensure data integrity and protection.**

KEY LEARNING POINTS



- The most important skill for e-transfers is partnership management with the service provider, in addition to strong competency in cash transfer programming in general.
- E-transfers require the development of new skills for beneficiaries who tend to feel more comfortable when they are supported by a trusted family member to conduct transactions.
- With e-transfers, training may be the single most critical investment to ensure beneficiaries remain in control of their entitlement.
- The process of transferring cash to beneficiaries should be mapped out with the finance team to ensure compliance with internal systems and donor requirements.
- Fraud mitigation and measures to deal with errors should be embedded in the e-transfer system and liability clearly defined in service contracts, should inconsistencies be found, but aid agencies should also develop their own internal risk controls.

I. IMPLEMENTATION SKILLS

There is a misconception that implementing e-transfer programmes requires outstanding technological skills from programme managers. The reality is that just a good understanding of the motivations and the internal functioning of the service provider, as described in [Section B-5](#), is often enough to successfully manage an e-transfer programme.

Key elements to consider

Partnership management: As mentioned, it is essential to develop a strong partnership with the service provider so that an adequate level of support is provided throughout programme implementation. In this respect, the most important skill to have is partnership management. A “win-win” situation occurs when both parties play to their respective strengths. A strong display of professionalism and being sensitive to the partners’ own challenges are beneficial to a healthy collaboration.

Technical expertise: Many aid agencies have found it useful to hire a technical expert to oversee their first ever e-transfer programme. Should the agency not be able to outsource this additional expertise, Table 10 presents the basic e-transfer orientation the cash programme manager should request from the service provider. Having said this, little can replace strong competency in cash transfer programming in general, because the key to a successful e-transfer intervention is good programme design, which incorporates remedial measures to the challenges encountered.

Table 10: Basic e-transfer orientation to request from service providers

Topics
• General introduction to the service (including the partners involved)
• Regulatory requirements and implications for beneficiary registration (including data disclosure practices)
• Using the online interface and making disbursements
• Hardware activation and distribution
• Using ATMs/PoS devices/working with agents
• Reconciliation
• Dealing with e-transfer recalls and errors
• Dealing with potential technical issues
• Frequently asked questions

2. BENEFICIARY TRAINING AND ENSURING ACCESS BY VULNERABLE GROUPS

E-transfers require the development of new skills by beneficiaries. As such, accompanying measures must be put in place to ensure access to the e-transfer service by the most vulnerable groups. A key challenge facing beneficiaries, as identified by many aid agencies which have used e-transfers, is **remembering and typing the PIN**.

Key elements to consider

Training methodology: Beneficiaries tend to favour peer training. Selecting a sub-group of beneficiaries who are slightly more comfortable with technology to train others using picture-based methodology, role plays and transaction simulations can prove successful. While the presence of service-provider personnel can be beneficial, it is often noted that they lack experience in appreciating the specific training needs of vulnerable groups.

Time and repetition: In addition to ensuring the appropriate training methodology is used, sufficient time must be allowed for the sessions which should be repeated as many times as necessary. Indeed, with e-transfers, training may be the single most critical investment to ensure beneficiaries remain in control of their entitlement.

“Helpers”: Using technologies, beneficiaries tend to feel more comfortable when they are supported by a trusted family member to conduct transactions. Agencies may fear that this would encourage PIN sharing and create risk for beneficiaries. Yet, anecdotal evidence indicates that, while voluntary password sharing creates a risk of theft, almost half of the people living in developed countries have done so once in their life with marginal negative impact on their personal finance. Should beneficiaries express the need to be supported by a trusted friend/family member, the aid agency must invite this person to attend the various training sessions to not only build his/her capacity to use the e-transfer device but also to sensitise him/her on their support function and the fact that they should not exploit the beneficiary.

Example from the field

BOX 16: MERCY CORPS PICTURE-BASED TRAINING (NEPAL)



In early 2013, **Mercy Corps** conducted a pilot in Nepal to provide assistance to some of Kathmandu's poorest residents and test digital vouchers that do not require negotiations with local MNOs or financial institutions. The objective was to identify quality voucher solutions that can be set up quickly in any location with basic mobile network connectivity (see Box 1).

To support the pilot, Mercy Corps developed the following training material in the local language.



Source: Murray, S. (2013) MasterCard Worldwide and Mercy Corps: ELEVATE Phase I Report. Mercy Corps.

3. MAKING E-TRANSFERS

Processes

The process of transferring cash to beneficiaries should be mapped out with the finance team to ensure compliance with internal systems.

Once beneficiaries have been selected and contracts have been negotiated, the process of electronically transferring cash to them is usually as follows:

Step 1	Load e-transfer disbursement account by bank transfer
Step 2	Log on to the web-based user interface for bulk payments
Step 3	Populate beneficiary name, phone number/card number etc.
Step 4	Enter transfer amount and frequency of transfers
Step 5	Verify the information
Step 6	Effect the transfer

Example from the field

BOX 17: CONCERN WORLDWIDE AND SAFARICOM PARTNERSHIP (KENYA)



Following the 2008 post-election violence in Kenya, thousands of households in the Tugen and Pokot communities of Kerio Valley in the Great Rift Valley lost their livestock and were displaced to less inhabitable areas. In response to this need, **Concern Worldwide** worked with a Safaricom team to specify and develop a tailored M-PESA (Safaricom's mobile money service) product to support these communities with cash transfers.

After technical and regulatory hurdles delayed programme implementation by about two months, Safaricom set up Concern as a corporate user of M-PESA, allowing the NGO to access and implement the service on a large-scale commercial basis.

Concern, as a corporate client, was given access to the M-PESA online interface, from which disbursements could be made. Concern transferred cash from its bank account into its M-PESA account, and paid service charges. Next, the list of beneficiaries was entered into a database that could be uploaded onto the M-PESA system. The key pieces of information contained in the database were beneficiary names, amounts due, and mobile phone numbers.

Once targeting was completed and the transfer system had been developed, teams from both Concern and Safaricom worked together to train the beneficiaries in the use of M-PESA, and to register them. Both teams travelled to the target area in early May 2008, where they spent about a week completing recipient registration processes and the first round of cash transfers.

Although considerable time was spent overcoming registration and technical challenges, this was essential for the success of the overall transfer process. The community engaged in the process of deploying the technology and adapted it to meet their needs and requirements. There was widespread satisfaction with the fact that money was made conveniently and safely available. This notably included older members of the community, who termed the ability to receive their entitlement through a mobile phone as a "miracle". The level of acceptance received by the response was an indication that adequate preparations had been made.

Source: Concern

BOX 18: (continued)



MerchantPRO Voucher System

The screenshot shows the MerchantPRO Voucher System interface. The main content area is titled 'REFILL VOUCHERS' and contains a table with the following data:

Voucher No.	Name	Phone	Status	Creation Date	Expiration Date
11112844	SHARLENE PRINCE 094	9799	0	28 Feb 2012 12:44:58	28 Mar 2012 12:44:58
11112845	WIDARJUNG CAHYA 094	9799	0002	28 Feb 2012 12:44:58	28 Mar 2012 12:44:58
11112846	JOSEPH ALEYS 094	9799	0000	28 Feb 2012 12:44:58	28 Mar 2012 12:44:58
11112847	LOUIS THOMAS 094	9799	0000	28 Feb 2012 12:44:58	28 Mar 2012 12:44:58
11112848	BENALICE WID 094	9799	0000	28 Feb 2012 12:44:58	28 Mar 2012 12:44:58
11112849	FRANCIS CHRY 094	9799	0000	28 Feb 2012 12:44:58	28 Mar 2012 12:44:58

M-PESA Mobile Money

The screenshot shows the M-PESA Mobile Money interface. The main content area is titled 'View recent Bulk Transaction Requests' and contains a filter form and a table of requests. The filter form includes fields for 'Start Date', 'End Date', 'Page Size', and 'Status'. The table has the following data:

ID	Scheduled Time	Status	Operator	Last Action By	Errors	Warnings
SR1	2008-12-11 11:20:00	Scheduled	mburic 000000	mburic manager	0	0

What it looks like in practice

Once a programme beneficiary has been registered on an e-transfer system, sensitised on programme objectives and trained on how to use the e-transfer device, he/she will go to a designated transaction point and carry out the e-transactions required to collect his/her entitlement.


Example from the field

BOX 19: MERCY CORPS MOBILE COMMERCE INFOGRAPHIC (HAITI)




Mercy Corps produced an infographic to illustrate a beneficiary user-experience with a mobile transfer, in the context of its cash-based interventions in the aftermath of the Haiti Jan 2010 earthquake.

1 ACCOUNT ACTIVATION
Marie, a Mercy Corps program participant, types in a code to activate her account and receives a message with her PIN. If her cellphone is lost or stolen, the PIN protects her account.




2 PAYMENT
Mercy Corps sends Marie an electronic payment.




3 OPTIONS
Now Marie has the option to:

- make purchases
- deposit money
- withdraw money
- transfer money
- store money safely


4 PURCHASE
Marie types in the code for "make a purchase" (123), her PIN, the vendor's phone number, and the amount of her bill.




Marie instantly receives a message with a unique transaction ID. She tells it to the merchant.



The merchant types in the code for "accept a purchase" (987), his PIN, the transaction ID, and the amount.



In seconds, both Marie and the merchant receive messages confirming the transfer of funds.



Source: Mercy Corps (2011) *Diary of a Mobile Money Program* | e-Book One: From Pilot Phase to Pilot Launch.

4. MITIGATING FRAUD RISKS AND DEALING WITH ERRORS

Fraud mitigation and measures to deal with errors should be embedded in the e-transfer system and liability clearly defined in service contracts, should inconsistencies be found, but aid agencies should also develop their own internal risk controls.

Key elements to consider

Funds traceability: In many respects, the use of e-transfers provides an added opportunity for the traceability of funds and reduces leakages.¹² Aid agencies can take a number of steps to carry out fraud verification. These can range from:

Degree of verification	–	<ul style="list-style-type: none"> • passively reviewing their disbursement account on the online interface for inconsistencies; • formally requesting individual balance check of beneficiaries from the service provider;
	+	<ul style="list-style-type: none"> • physically collecting receipts from merchants (in a voucher programme); • actively conducting interviews and surveys with a sample of beneficiaries.

Communication with beneficiaries: Mobile phones can also be used to communicate entitlements to recipients prior to the transfer and to gather feedback/complaints afterwards (via phone calls or SMS).

Error correction: As user-friendly as e-transfer systems may be, human error can never totally be avoided. The mistake most likely to happen is making an e-transfer to the wrong SIM/voucher/card. Different service providers will have different ways of addressing this. But often when the service provider is a bank, there is a slightly more complex process of transaction recall because of prudential laws on accessing personal accounts (even virtual ones). Aid agencies should enquire about this when signing a service contract and ascertain where potential liabilities lie.

Error documentation: Procedures for reporting errors to the service provider can also be useful as error logs can provide valuable monitoring and evaluation data, helping the aid agency determine the source and frequency of issues encountered.

Internal fraud: Measures should also be put in place to protect against internal fraud.

Additional guidance

A fraud and corruption risk mitigation template is provided in [Section E-8](#).

¹²Smith, G., MacAuslan, I., Butters, S. and Tromme, M. (2011) *New Technology Enhancing Humanitarian Cash and Voucher Programming*, a research report commissioned by CaLP.

SECTION D: COMPLIANCE, MONITORING AND EVALUATION, DATA PROTECTION AND COMPLAINTS

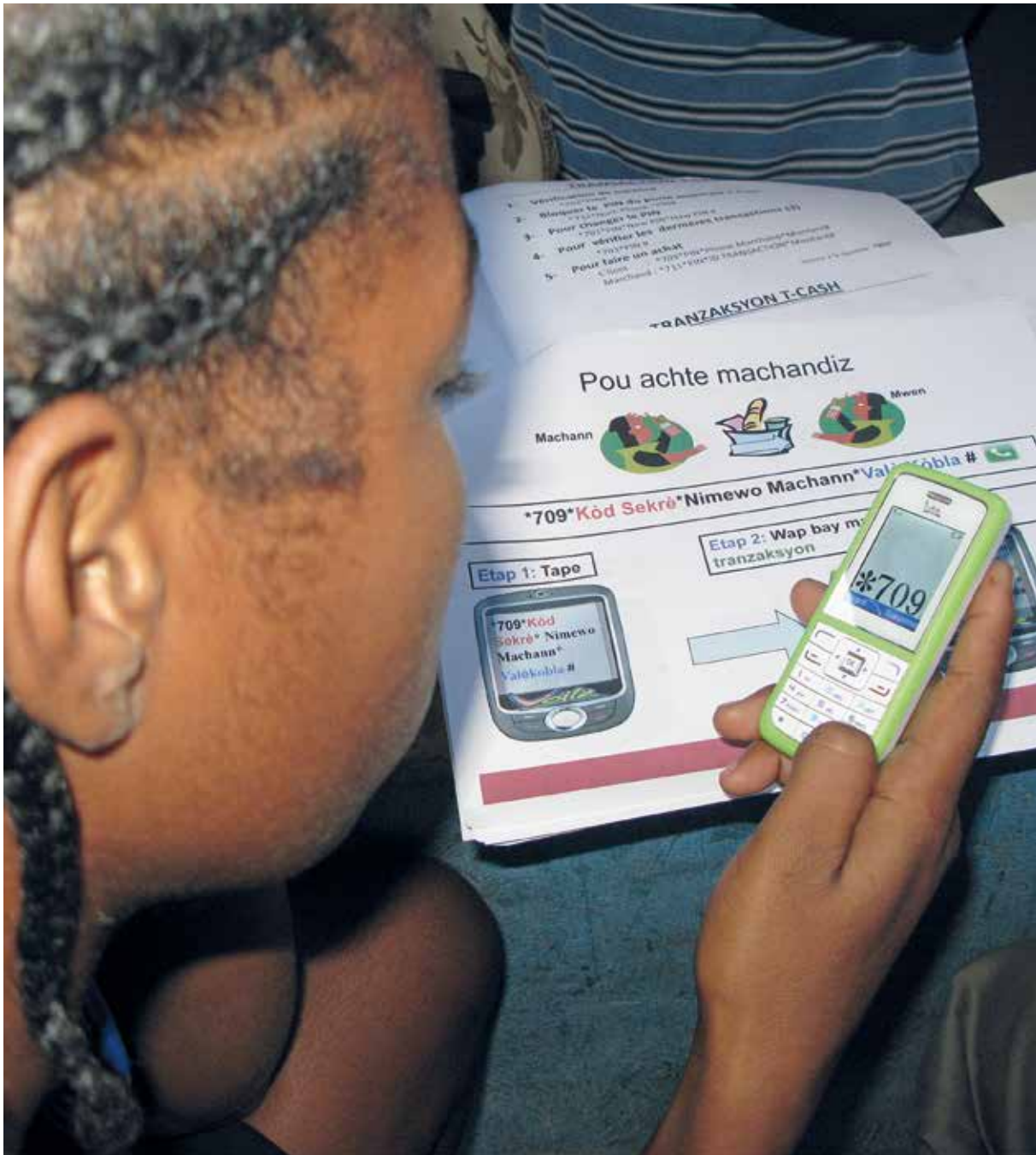


PHOTO: ERIN WILDERMUTH/MERCY CORPS

This section addresses questions of compliance with internal policies, procedures and systems as well as **donor and legal requirements** when choosing to use e-transfers. Attention is paid to the **monitoring and evaluation process** as well as ways in which to **ensure that beneficiary data is protected and complaints are handled appropriately**.

KEY LEARNING POINTS



- Aid agencies should be prepared for the fact that e-transfers can raise issues which can affect their existing financial controls and may warrant reviewing and amending internal processes as well as requiring service providers to adhere to the agency's standards.
- Whilst to a great extent, monitoring and evaluation (M&E) can be aided by e-transfer systems, because of the computer-based reports that can be generated, aid agencies still need to have strong M&E processes in place.
- However attractive an option e-transfers can be, if aid agencies cannot guarantee the protection of beneficiary data, e-transfers should not be considered.
- The support provided by commercial helplines and other customer services does not preclude aid agencies from setting up their own feedback/complaints mechanism, not least because beneficiaries may want to raise confidential concerns about staff of the service providers or the aid agency itself.

I. COMPLIANCE

E-transfers can raise issues which can affect an aid agency's existing financial controls and may warrant reviewing and amending internal processes as well as requiring service providers to adhere to the agency's standards.

Compliance concerns are best addressed as part of preparedness plans, when considering e-transfer options ahead of an emergency.

Key elements to consider

Proof of receipt – did the beneficiary receive the e-transfer?: In manual cash transfers, beneficiaries offer a signature or a fingerprint as proof of cash collection. With e-transfers, online interfaces can generate reports documenting that the aid agency's master account was indeed debited to credit the accounts/phone numbers of the intended beneficiaries. But actual confirmation on the beneficiary side may not always be readily available from the online interface. Although this information can be obtained from the service provider, it raises an issue of breach of privacy when beneficiaries have not given prior consent to aid agencies to view their account balance.

Authentication – was it the intended beneficiary who collected the e-transfer? : Again, e-transfer online interfaces can generate reports indicating how much cash was transferred to which account/phone number and when. The challenge is that they may not always be able to document whether the beneficiary to whom cash was transferred did collect the cash. When phones are shared in a mobile transfer programme, it is even more difficult to ascertain the identity of the person collecting the cash. This raises the question: is a four-digit PIN sufficient for authentication, or is additional authentication necessary (i.e. through checking a photo ID or through biometrics) to protect beneficiaries?

Accessibility challenges – how can the use of “helpers” be accommodated?: When beneficiaries are unable to engage with technology independently (for example, enter a four-digit PIN), they may rely on the support of a trusted family member or friend (as described in [Section C-2](#)). Some programmes have effectively registered both the helper and the beneficiary and post-distribution monitoring (PDM) was conducted to ensure the intended beneficiary effectively collected his/her entitlement.

Segregation of duties – who should do what?: In most e-transfer systems, there is only one user-type with full privileges ranging from viewing and populating beneficiary data to effecting transfers. As beneficiary information often resides with programme teams, this may be a concern for agencies which typically like to devolve any payment function of the finance department. In addition, aid agencies' finance processes generally assign a minimum of two signatories for cheques and account transfers. If tiered privileges (such as maker, checker and reviewer) are not available in the e-transfer system, the person who enters beneficiaries' data and entitlement in the system may also be the one effecting the payment.

Merchant reimbursement (in voucher programmes): The requirements for payment verification information must be clear. What level of information on the type, quantity and costs of goods delivered to beneficiaries through local merchants is required to reimburse merchants? Should the programme solely rely on electronic transactions or should paper files be requested to verify transactions?

Reporting: Aid agencies and their donors may have very strict reporting requirements. What reporting formats are acceptable to donors and to meet internal requirements? Are print-outs from the online interface accepted in CSV format or is PDF format preferred? Do cash disbursement reports need to bear the logo and the stamp of the service provider?

As e-transfers are new and rapidly evolving, many donors and organisations have yet to establish clear guidance for many of these compliance issues. **In these contexts, it is advisable to agree on minimum standards for verifying beneficiary cash collection with auditors and donors before the programme starts.**

2. PROGRAMME DESIGN, MONITORING AND EVALUATION

Whilst to a great extent monitoring and evaluation (M&E) can be aided by e-transfer systems, because of the computer-based reports that can be generated, aid agencies still need to have strong M&E processes in place.

Key elements to consider

Beneficiary targeting: In the design phase, as with all humanitarian interventions, targeting the right beneficiaries from the outset is clearly essential. Organisations should bear in mind that the use of both new technology and cash transfers is extremely attractive to communities and there can be inclusion/exclusion errors on beneficiary registration lists. However secure the delivery mechanism is, it will likely never be a substitute for effective beneficiary selection and monitoring procedures. Clear beneficiary selection processes, verification, monitoring and complaints mechanisms must always be put in place.

Exclusion: Extra care must be taken to frequently assess that the use of technology is not inadvertently excluding vulnerable participants. For example, if mobile phones are required, are there procedures in place to accommodate beneficiaries that do not have access to a phone? Is community selection being unduly affected by technology criteria, as compared to vulnerability criteria? Are vulnerable communities not selected due to lack of mobile signal or electricity? If beneficiaries need assistance to complete e-transfers, is support available? Programme design and monitoring should routinely assess if the most vulnerable populations are included and have full access to programme benefits and services.

User experience and service quality: During programme implementation, the M&E process should capture beneficiaries' experience with e-transfers in terms of ease of access to the funds. Aid agencies should conduct regular spot checks to identify any emerging issues as full post-distribution monitoring (PDM) may take time to analyse. They should also inquire about liquidity at the agent, level of customer service at agent/merchant, average transaction time and ATM/PoS functionality. If difficulties are noticed, they should investigate whether additional training and/or service provider intervention is required.

Funds traceability: Because e-transfer systems do not track the use of funds but value transfer, there is still a need to conduct on-site and post-distribution monitoring. The first concern is ensuring that beneficiaries have been paid in the first place. This is easily done by accessing the e-transfer online interface. In addition, aggregate or individual account information can also be requested from the service provider, provided beneficiaries have consented to this.

Sampling and reconciliation: Aid agencies new to e-transfers have often commented on the excessive burden of monitoring because additional care is put in to ensure compliance from both the service provider and agents/merchants. Random sampling of beneficiaries to find out how they used their e-transfer may include phone/SMS interviews when mobile transfers are used. Reconciliation of merchant receipts and triangulation with the service provider on the amount paid to merchants (if applicable) can also be conducted. Arguably, the use of e-transfers should not preclude merchants from keeping paper receipts of the transactions they conducted, in case of dispute.

Indicators: At a minimum, monitoring should include collecting data on (1) process indicators and (2) impact indicators. Additionally, aid agencies can develop monitoring tools to ascertain that beneficiaries were able to complete the transaction independently, that they retained control of the purchase (including deciding what, when and where to buy, and maintaining control over items once bought) or their cash collection. They can seek to identify power dynamics in the household to understand the impact of the e-transfer mechanism.

Additional guidance

Sample PDM tools are provided in Section E-9.

3. DATA PROTECTION

As mentioned in the introduction, these *E-transfers Implementation Support Guidelines* form part of a three component research launched by CaLP in early 2013.

Another key output of this research is *Protecting Beneficiary Privacy: Principles and Operational Standards for the Secure Use of Personal Data in E-Transfer Programmes*, which focuses on the **protection of beneficiary personal data**, broadly defined as any data that can be used to identify an individual by virtue of the information it contains.

Although many developing countries are still in the process of developing comprehensive client protection legislation, aid agencies engaged in e-transfers and their partners should put in place measures to ensure the protection of beneficiary data through specific data protection clauses which address the privacy-related risks of cash transfers in their service contract.

These risks are associated with the inappropriate collection, use, storage, disclosure and disposal of the personal data of beneficiaries. This is a particular concern given the web of actors that aid agencies are required to deal with to process e-transfers for their beneficiaries. Yet, in an online survey initiated by CaLP in May 2013 which collected feedback from 52 respondents in the cash transfer community of practice, 61.5% of the respondents reported that their organisation does not have internal data management guidelines.

Key elements to consider

Data ownership: Beneficiaries remain the sole owner of their personal data. Their right of access to the data collected from them by an aid agency, and the means of exercising this right freely must be communicated to them clearly.

Informed consent: Aid agencies request informed consent from beneficiaries when collecting their personal data and explain to them why this data is collected and its intended use. Alternative transfer mechanisms should be put in place if beneficiaries are unwilling/unable to provide that consent.

Purposeful collection: Whilst bearing in mind that a commercial relationship is created between the service providers and the beneficiary as soon as he/she receives an e-transfer device, aid agencies should ensure that beneficiary data collected for e-transfers is used for that purpose only. Renewed consent should be sought from beneficiaries if this purpose changes.

Storage and security: Beneficiary data should be securely stored with restricted access. Agencies should make it clear who in their organisation is responsible for data security. They should put processes in place for the protection of beneficiary personal data from loss, theft, damage or destruction, including back-up systems and effective means to respond to security breaches.

Disclosure: The organisations with which the service provider intends to share beneficiary data provided by the aid agency must be listed exhaustively. The service provider must accept liability for any inappropriate use of beneficiary data by its own organisation as well as those to which it discloses beneficiary data.

Disposal: It should be made clear how beneficiary information will be disposed of at the end of the programme. In some countries, this data may be owned by the government. Aid agencies must make sure that this does not represent protection risks for the recipients.

Content: With regards to type of data that needs to be collected, aid agencies are reminded not to be excessive and focus solely on what is required to meet KYC procedures (see [Section B-6](#)).

However attractive an option e-transfers can be, if aid agencies cannot guarantee the protection of beneficiary data, e-transfers should not be considered.

Additional guidance

A plain language template for collection of beneficiary consent is provided in [Section E-10](#), and sample data protection clauses to include in service contracts in [Section E-11](#).

Additional guidance of all issues relating to protecting beneficiary personal data can be found in CaLP (2013) *Protecting Beneficiary Privacy: Principles and Operational Standards for the Secure Use of Personal Data in E-Transfer Programmes*. A copy of the principles is provided in [Section E-12](#).

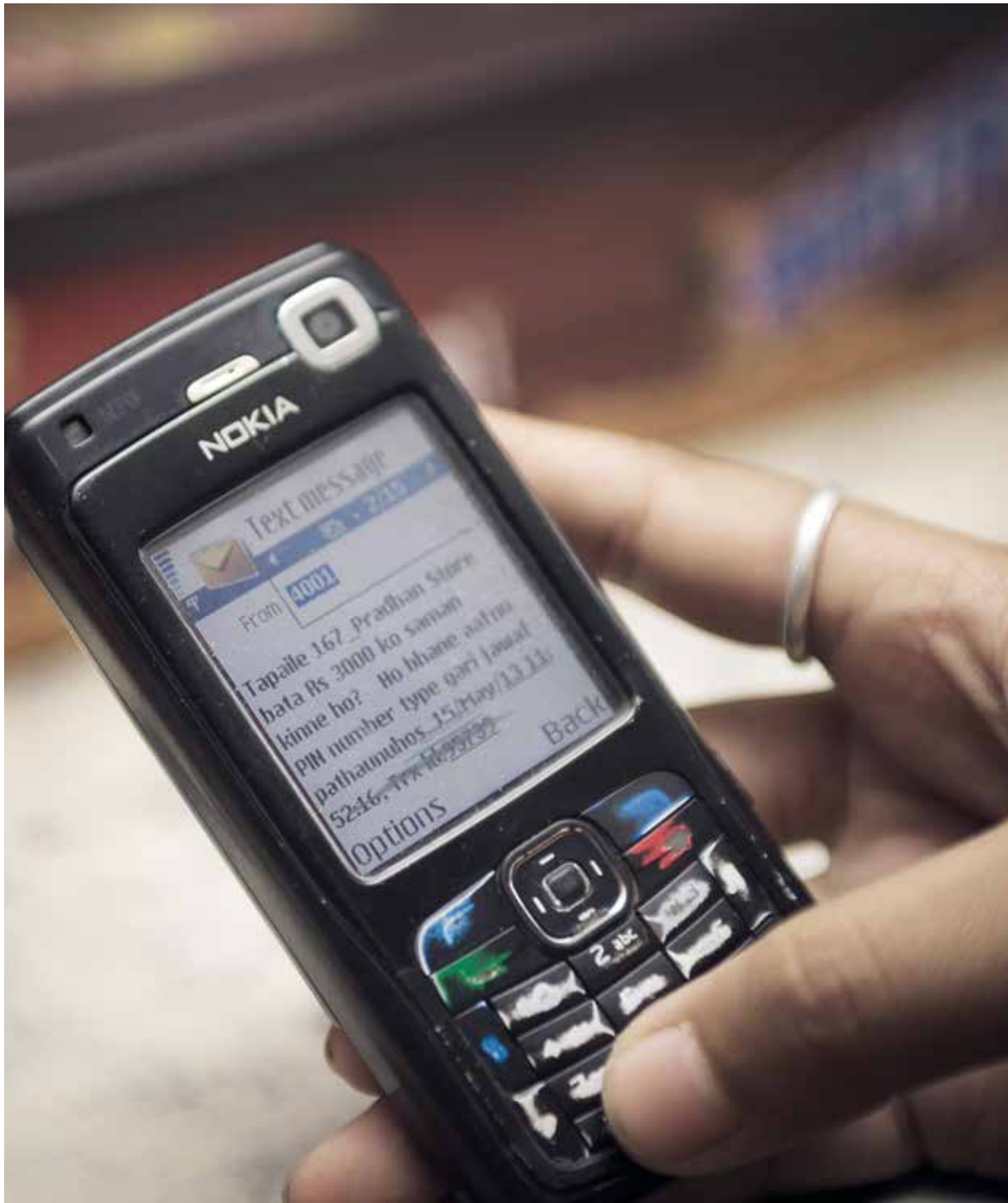


PHOTO: SURAJ SHAKYA

4. COMPLAINTS MECHANISMS

Many agencies express concerns over the fact that e-transfers create distance between them and their beneficiaries. Since e-transfers do not imply physical direct distribution, physical presence of the aid agency staff in the project area may be considerably reduced. The positive side of this is that it frees up more time for aid agency staff to conduct monitoring activities and reinforce the complaint and feedback mechanism they have in place with beneficiaries to make sure participants and non-participants have a way to communicate easily and regularly with the programme staff.

Key elements to consider

Hotlines: E-transfer services include a customer service hotline which beneficiaries can access by phone or SMS. Assistance is also provided at the retail location of the service providers, and sometimes at the agents. This commercial support does not preclude aid agencies from setting up their own feedback/complaints mechanism, not least because beneficiaries may want to raise confidential concerns about staff from service providers or from the aid agency itself.

Customer service: Attention must be paid to capturing customer service related complaints and system failures as well as issues related to the programme itself (including programme staff). To avoid any confusion, it must be made clear to beneficiaries which services are offered by the service provider and which are offered by the aid agency, hence the confidentiality of the respective complaints mechanisms.

Communication with beneficiaries: Mobile phones are often cited as a useful tool for two-way communication and dialogue with beneficiaries, and can be used for sensitisation and accountability to beneficiaries.

Example from the field

BOX 20: DRC SMS FEEDBACK SYSTEM (GLOBAL)



In September 2011, the **Danish Refugee Council** (DRC) launched the “SMS Feedback Project”, an accountability system for the delivery of humanitarian aid in Somalia using SMS feedback and social media.

The project gathers feedback from beneficiaries using SMS via a local SIM card, and posts the translated and uncensored feedback on the webpage somcdrc.org/hif. In addition, findings are shared using a number of social media – including Twitter, Facebook and through a blog.

Increasing numbers of communities in Somalia where the Danish Refugee Council provides humanitarian assistance are using the SMS feedback system to lodge complaints and tell when something is wrong. One example from Mogadishu in Somalia shows how the SMS system can be used to track unexpected mistakes – in this case the complaint was first seen as a lack of aid from the Danish Refugee Council.

“My cash collection ID card was taken by force by one of your staff in the Mogadishu office when I went to collect monthly cash payments. I want to know why he took my card and would like your help in getting it back. The staff who took my card accused me of having a duplicate card, which is untrue.”

The SMS feedback team on the ground looked into the case and soon the investigation identified the problem which was then filed in their report and explained to the man who sent the SMS. “This man has two ID cards for one family, because his wife and he applied as 2 separate families. His wife has recently passed away and he has been collecting her cash as he is her next of kin.”

To ensure transparency, all SMS complaints and feedback are translated and anonymised and then shared on social media, allowing a wider audience to have access to the information and to engage in dialogue.

Source: <http://drc.dk/>

SECTION E: ADDITIONAL GUIDANCE



PHOTO: SURAJ SHAKYA

This section presents a number of **tools** to support agencies using e-transfers.

Content

1. Cash transfer programming reference document
2. Procurement process for an e-transfer service provider
3. Prerequisites for selecting an e-transfer service provider
4. Cash emergency preparedness risk assessment
5. Sample mobile usage and awareness questionnaire
6. Interview guide/checklist of key issues with service providers
7. Minimum contract requirements with an e-transfer service provider
8. Fraud and corruption risk mitigation template
9. Sample-post distribution monitoring (PDM) tools
10. Sample data protection clauses: Beneficiary notice and consent
11. Sample data protection clauses: Aid agency and e-transfer service provider
12. Data protection principles

I. CASH TRANSFER PROGRAMMING REFERENCE DOCUMENT

Resource	Publishing agency
Cash transfer guidelines and tools	
Good Practice Review 11: Cash transfer programming in emergencies	Humanitarian Practice Network, ODI (2011)
The Use of Cash and Vouchers in Humanitarian Crises	DG ECHO (2013)
The Sphere Project (Chapter 4.3)	The Sphere Project (2011)
Delivering Money	CaLP (2010)
The Use of Cash and Vouchers in Humanitarian Crises. DG ECHO Funding Guidelines	DG ECHO (2009)
Cash and Vouchers Manual	World Food Programme (2009)
Guidelines for Cash Transfer Programming	International Red Cross and Red Crescent Movement (2007)
Cash Workbook: A practical user's guide for the preparation and implementation of cash projects	Swiss Agency for Development and Cooperation (2007)
Implementing Cash-Based Interventions	Action Contre La Faim (2007)
A Practical Guide for Cash-Based Response in Emergencies	Horn Relief (2007)
Cash-based Responses in Emergencies	Humanitarian Policy Group, ODI (2007)
Cash-Transfer Programming in Emergencies	Oxfam (2006)
Voucher programming	
Agriculture in emergencies: Guidelines on the use of seeds, fertilisers and cash	British Red Cross (2000)
CRS Seed Voucher and Fairs: Using Markets in Disaster Response	Catholic Relief Services (2004)
Implementing Cash-Based Interventions	Action Contre La Faim (2007)
Cash for work	
Cash For Work programming: A practical guide	Oxfam (2002)
Guide to Cash-for-Work Programming	Mercy Corps (2006)

Adapted from Harvey and Bailey (2011) *Good Practice Review 11: Cash transfer programming in emergencies*. Humanitarian Practice Network. ODI.

2. PROCUREMENT PROCESS FOR AN E-TRANSFER SERVICE PROVIDER

MAIN STEPS	LEADING DEPARTMENT	SUPPORTING DEPARTMENT
Procurement planning	Logistics	Technical
Procurement request + criteria for selection	Technical	Administrative (especially if banks are involved and administrative criteria need to be considered)
PFU integration + PD reference creation	Logistics	
Purchase process ↳ Call for interest Transfer service Provider selection Provider selection agreement	Logistics Logistics Logistics	Administrative and Technical Administrative and Technical through evaluation/ selection committee Administrative leads negotiation with financial institution, supported by Technical
Delivery of cash	Administrative	Technical
Payment of transfer service	Administrative	
Archiving	Administrative and Logistics	

Source : ACF (2012) *Logistics and Administration Guideline For Cash Based Interventions*

3. PREREQUISITES FOR SELECTING AN E-TRANSFER SERVICE PROVIDER

Prerequisites for selecting an e-transfer service provider (card/mobile phone)	Comments	✓
1. There is a reliable and accessible mobile phone network within the project target zone		
2. The platform for bulk payments can manage the number of transfers required		
3. The service provider is able to provide dedicated service support to the aid agency		
4. The service provider is able to encrypt the data between the aid agency and mobile phone company		
5. The agent distribution network aligned with the service provider has sufficient liquidity to deal with the cash demands of the beneficiaries		
6. The agent distribution network is close enough to the beneficiaries to enable distribution without significant cost to the beneficiary		
7. The commission/service charge for providing the transfer service is acceptable		
8. The charge to beneficiaries for accessing their cash at the agents is acceptable		
9. Beneficiaries have access to mobile phones/cards or can be provided with them quickly		
10. Beneficiaries have enough knowledge to use the system or can quickly be supported to do so		
11. Beneficiaries have the ID that is required for registration to the service		
12. Beneficiaries using mobile money have or can be provided with cost-effective access to a source of power to keep phones charged		
13. Data protection policy is in place governing management of beneficiary data		
14. Compliance with internationally-agreed counter-terrorism measures (lists of restricted persons and individuals) is assured		
15. There is protection for the aid agency in the event the provider becomes insolvent, such as ring-fencing of funds transferred.		

Adapted from Concern Worldwide

4. CASH EMERGENCY PREPAREDNESS RISK ASSESSMENT

The table below summarises the stages of the Cash Emergency Preparedness (CEP) risk assessment; the key questions to be answered at each stage, and the recommended approach at national level and field level.

Cash Emergency Preparedness (CEP) risk assessment	
1. Appropriateness	
QUESTION: Is CTP politically/socially/culturally acceptable to communities and within the local context? Can CTP be used to meet the most likely emergency-related needs? What CTP modality may be most appropriate to meet needs?	
APPROACH (at national level): Stakeholder analysis including: <ul style="list-style-type: none"> • Donor positioning on CTP in country and in the region • Experience of other agencies/institutions implementing CTP • Experience of government-led social protection cash programmes • Beneficiary acceptability 	APPROACH (at field level): <ul style="list-style-type: none"> • Vulnerability analysis for key sectors likely to use CTP as an emergency response tool • Assessment of needs to be addressed through CTP including scope and scale and value of potential transfers • Beneficiary acceptability at local level
2. Market feasibility and trends	
QUESTION: Is CTP logistically possible, timely and cost effective to meet the potential needs of beneficiaries? Will CTP impact positively on beneficiaries/communities and markets in the long term?	
APPROACH (at national level): <ul style="list-style-type: none"> • Analysis of national level market trends for the key commodities/services likely to be required in an emergency • Overview of national market recovery trends after previous emergencies 	APPROACH (at field level): <ul style="list-style-type: none"> • Market assessment for key commodities identified through vulnerability analysis • Local level market trends for key commodities/services likely to be required in an emergency • Understanding of local market recovery trends after previous emergencies
3. Finance	
QUESTION: Is there an appropriate delivery mechanism which ensures speed and accountability, while reaching all vulnerable groups? This stage should also include an assessment of logistical and finance capability in terms of ensuring security and accountability.	
APPROACH (at national level): <ul style="list-style-type: none"> • Overview and analysis of CTP delivery mechanisms available in country • Experiences of delivery mechanisms by other agencies • Opportunities for public/private partnerships and updates on development of new technologies 	APPROACH (at field level): <ul style="list-style-type: none"> • Understanding of local market recovery trends after previous emergencies • Experiences of delivery mechanisms by other agencies • Identification of one delivery mechanism to scale-up in case of an emergency • Identification of one contingency mechanism if first choice delivery mechanism fails
4. Security	
QUESTION: Is the proposed delivery mechanism safe for agency staff and beneficiaries?	
APPROACH (at national level): <ul style="list-style-type: none"> • Analysis of national-level security implications of CTP implementation 	APPROACH (at field level): <ul style="list-style-type: none"> • Detailed local implications of implementing CTP through chosen delivery mechanism • Identification of potential risks and recommendations on how these can be mitigated against

Source: Save the Children (2013) *Cash Emergency Preparedness (CEP) planning – Guidelines and key findings from pilot assessments*. London: Save the Children

5. SAMPLE MOBILE USAGE AND AWARENESS QUESTIONNAIRE

<p>40. Do you own a mobile phone? 1. Yes CONTINUE 2. No GO TO 54</p>	<p>41. Do you know how to send SMS/texts? 1. Yes 2. No</p>
<p>42. Do you know how to receive SMS/texts? 1. Yes 2. No</p>	<p>43. Are you able to make and receive calls on mobile phone? 1. Yes 2. No</p>
<p>44. Do you have access to the internet on your mobile phone? 1. Yes CONTINUE 2. No GO TO 46</p>	<p>45. Do you know how to operate the internet on your mobile phone? 1. Yes 2. No</p>
<p>46. Do you receive cocoa market price information on your mobile phone? 1. Yes 2. No</p>	<p>47. Do you know how to check your airtime balance? 1. Yes 2. No</p>
<p>48. Where do you buy airtime? 1. Grocery store in the neighbourhood 2. Airtime seller in the neighbourhood 3. Any other (Please specify....)</p>	<p>49. How much airtime do you generally buy in a month? Please input the number. _____ Amount (in '000s)</p>
<p>50. Who is your network provider? 1. Telkomsel 2. Indosat 3. Axis 4. XL 5. Any other. Please specify</p>	<p>51. How reliable is the service from your mobile network operator? 1. Excellent 2. Very good 3. Good 4. Poor 5. Very poor</p>
<p>52. In the past 12 months, have you used a mobile device to? 1. Pay bills CONTINUE 2. Send money CONTINUE 3. Receive money CONTINUE 4. No GO TO 58</p>	<p>53. How far are you located from a service point (the place where you do the cash deposit and cash withdrawal transactions)? 1. <1km 2. 1-5km 3. >5km</p>

(continued from page 72)

<p>54. Does someone else in your family own the mobile phone? 1. Yes CONTINUE 2. No GO TO 57</p>	<p>55. Do you share the mobile phone with that family member? 1. Yes CONTINUE 2. No GO TO 57</p>
<p>56. Do you/they use multiple SIM cards? 1. Yes 2. No</p>	<p>57. Why don't you use the mobile phone? 1. Don't know how to operate it 2. Don't have enough money to buy a mobile phone/ It is expensive 3. It is time consuming 4. Any other. Please specify</p>
<p>58. Are you willing to use your mobile phone for transactions like bill payments, money transfer/ remittance, purchase airtime, loan repayment, etc.? 1. Yes CONTINUE 2. No GO TO 62</p>	<p>59. What benefits do you see of using the mobile phones for financial transactions? (No more than two answers permitted). 1. Save time/convenient 2. Save transport cost 3. More secure transaction 4. Faster transactions 5. Ability to save and earn interest 6. More private 7. Fewer risks (than carrying cash in hand, etc.) 8. Lower cost 9. Other. Please specify 10. I don't know</p>
<p>60. For the services you normally use at a bank (deposit/withdrawal, transfer money, bill pay, receive salary or other money, buy airtime), would you be willing to use an agent, such as an agri-input supplier, post office, fuel station, or merchant rather than a bank to access these services? 1. Yes CONTINUE 2. No GO TO 62 3. I don't know GO TO 62</p>	<p>61. At which of these places would you be willing to undertake mobile money transactions? 1. A large agri-input dealer 2. A fuel station 3. Local supermarket 4. Airtime dealer in the neighbourhood 5. Trader/collector 6. A microfinance institution 7. A bank branch or other bank outlet 8. Local cooperative institution 9. ATM machine 10. Other (please specify) 11. Don't know 12. Refused</p>
<p>62. Can we contact you for follow-up interviews? 1. Yes CONTINUE 2. No GO TO End time</p>	

 Source: USAID (2013) *Market Insights Into The Financial Behaviors And Design Of Mobile Financial Services Products For Cocoa Farmers In Indonesia.*

6. INTERVIEW GUIDE/CHECKLIST OF KEY ISSUES WITH SERVICE PROVIDERS

Date		Interviewee	
No	Key Issue	Question	Answer
1	Experience	Has your organisation had previous experience with cash payments to victims after emergencies?	
2	Future involvement	If the answer to Question 1 is no: would you be interested in possible future involvement?	
3	Time period	If the answer to Question 1 is yes: please describe this experience. Is this experience historic (e.g. a completed project) or ongoing?	
4	Method of transfer	If the answer to Question 1 is yes: how was the cash transferred? ¹³	
5	Frequency of payments	If the answer to Question 1 is yes: was the cash transferred in a lump sum or in a number of payments?	
6	Stakeholders	If the answer to Question 1 is yes: what parties were involved in the cash transfer process? ¹⁴	
7	Delivery points	Does your institution have existing delivery points in potential needy areas and if so can you provide a map showing them?	
		If not how would you roll them out rapidly and robustly?	
		Do you already have the required technology or would you need to implement or adapt, and how long would this take?	
8	Role	How would you see your role and how would you deliver cash to disaster survivors in a given context? (e.g. in addition to the core business, would you see a role in, for example, fraud controls, security, training, IT, management reports, communications and reconciliations?)	
9	E-transfer device	What type of e-transfer devices could be used to provide cash payments in emergency contexts?	
		Are these e-transfer devices already in place or would there need to be any further development and, if so, what would be the time and cost implications?	
		<i>(Where previous experience exists, what type of e-transfer devices were used?)</i>	
10	Reporting	What reports would you be able to provide to an aid agency, and within what time period? For example, reconciliations of money received and money withdrawn, money in wallets.	
		<i>(Where previous experience exists, what type of reports were provided?)</i>	
11	Assessment of delivery options	What would the criteria for selection of the solution for delivery options be in terms of delivery points and e-transfer devices?	
		<i>(Where previous experience exists, what was the process for assessing delivery options?)</i>	
12	Communication	Does your institution have experience of communicating effectively with this market segment to explain how to use the selected payment channels? ¹⁵	

¹³ E.g., direct delivery by agency, direct delivery by sub-contracted private sector actor such as a bank or remittance company, government offices or other parastatal distribution points, indirect delivery via e-transfer devices to offices of the above or via other agency points.

¹⁴ E.g., agency plus bank or remittance company, security company, strategic partners possibly in other countries, etc.

¹⁵ E.g. does the institution have experience of financial literacy training in order to be able to effectively explain the use of the selected e-transfer devices to the recipients?

(continued from page 74)

No	Key Issue	Question	Answer
13	Costs of delivery mechanism for the aid agency (allocation of roles and responsibilities)	How would you structure your charges to an aid agency for the mechanism for the delivery of cash?	
		What would the costs of the chosen delivery mechanism for the aid agency be in terms of: <ul style="list-style-type: none"> • Charges by the provider (e.g., % fee charged by you)? • Set up costs charged by you? • Security? • Education and training? 	
		What would you see as a reasonable % benchmark in different contexts?	
		<i>(Where past experience exists, what were these costs/ how were charges to aid agencies structured?)</i>	
14	Costs of delivery mechanism for the recipients	How would you structure the charges for this service? What would the costs of the chosen delivery mechanism for the recipients be in terms of: <ul style="list-style-type: none"> • Any charges – e.g. bank charges for individual accounts? • Travel time and costs to and from where money is distributed or collected? • Waiting times at the distribution point? 	
		<i>(Where previous experience exists, what were these costs?)</i>	
15	Basis for costs	How would these costs relate to other payment services you offer? E.g. to pensioners, mass market.	
16	Cost containment	How could we work to minimise costs? E.g. upfront investment, involvement of strategic partners, outsourcing.	
17	How would your solution rate in terms of the following criteria?	How would the proposed chosen delivery mechanism rate in terms of: <ul style="list-style-type: none"> • Reliability – recipient ability to receive cash as expected? • Resilience – ability of mechanism to cope with the disruption of a disaster and with changing circumstances, e.g. more recipients, changing locations? • Accountability – corruption risks associated with the mechanism? • Other control issues? • Security – safety of recipients while receiving the cash? • Vulnerable groups – any issues particular to vulnerable groups (such as women or children) associated with the mechanism? 	
		<i>(Where previous experience exists, how did the chosen delivery mechanism rate in terms of the above criteria, and where there were any challenges, how were these dealt with?)</i>	
18	Organisational	Does your institution have a specific function or department that would handle such a function? Would this be at the country, regional or other international level? Where would the initial entry point be for an agency to enter into discussions with your institution?	
19	Form of relationship	Would you see this as an ad hoc project or as a possible ongoing relationship with one or more aid agencies on a regional or multi-country basis? If long term, what additional added value could you provide in terms of, say, contingency planning, or improved pricing as a preferred supplier?	
20	Rapid delivery	What would you see as the most effective way of speeding up the delivery of cash to recipients after an emergency?	
21	Motivation	What would be the motivation for your organisation to be involved in this business?	
		Are there certain contexts where you see particular potential for involvement?	
22	General	Any other comments?	

Source: Harvey, P., Haver, K., Hoffman, J., Murphy, B. (2010) *Delivering Money. Cash Transfer Mechanisms in Emergencies*. CaLP

7. MINIMUM CONTRACT REQUIREMENTS WITH AN E-TRANSFER SERVICE PROVIDER

At a minimum, a contract with a service provider must include:

- Outline of the period covered by the agreement.
- Operation of service outlining the roles of the service provider – including controls to follow; any equipment or e-transfer devices to be provided; any role in registration; activation of accounts; process for the transfer of funds to recipient and reporting; notifying beneficiaries; any training of staff/beneficiaries; any informing of service agents/branch staff within the project zone about the programme and required liquidity; any aids to visibility for recipients; customer services support provided in the event of service failure.
- Outline of the role of the aid agency including any training, registering of beneficiaries, providing beneficiary list and finances to the service provider in timely fashion, ensuring correct ID, and following the controls set by the service provider (e.g. for web-based access to an account).
- For new and pilot initiatives, inclusion of a termination clause, or pilot phase within which early termination by either party is possible.
- The location and number of distributors/agents/branches.
- Details of what constitutes force majeure.
- Expected duration of set-up phase including any testing.
- Details of the payment schedule including time that any e-transfer devices (e.g. cheques/bank cards) will be provided to the aid agency; that funds and any advance charges will be provided to service provider; and time by which service providers must fulfil their disbursement role.
- Detail of dedicated staff for the project.
- Aid agency's transaction and account limits, and those of beneficiaries where relevant.
- Maximum number, and value, of beneficiary payments that can be made per day.
- All the transaction charges including any waivers from normal charges.
- Grievance/troubleshooting procedure.
- Any special relaxations/considerations.
- Security arrangements the service provider must have in place – e.g. armoured vehicles in the case of courier services; secure SMS transactions in the case of mobile money transfer.
- Insurance against loss or against insolvency.
- Data protection requirements.
- Details of the verification criteria and documentation process the service provider must follow when transferring cash to beneficiaries.
- Details of the reporting requirements including frequency, content and proof of transaction. This may include procedures for access to any online web portal of the aid agency and beneficiary accounts hosted by the service provider.
- Details of the commission accruing and the terms under which the service provider will be remunerated (likely to be on a monthly basis upon completion of activities as verified through completed reporting and monitoring, through bank transfer).
- Outline of the process to follow for absentees, bounce-backs and repayments.
- Clear penalties especially around inability to supply agreed goods.
- Clauses detailing the aid agency's position on fraud and programme participant protection, and responsibilities of the service provider.
- Clauses detailing procedure for the protection of beneficiary personal data.
- Exit strategy including any account de-activation periods and additional support from the service provider beyond the transfer period.

8. FRAUD AND CORRUPTION RISK MITIGATION TEMPLATE

Programmatic Phase	Risk	Mitigation
Assessment/ Targeting	<p>Fraud: Inaccurate information that leads to inappropriate prioritisation</p> <p>Political Corruption: Government officials direct agencies to the “most affected areas” within their constituencies</p>	<ul style="list-style-type: none"> • Clear targeting criteria • Use of different teams to target, distribute, and verify • Independent assessments by NGOs to verify government-provided lists and assessment information
Beneficiary Selection	<p>Fraud: Registration of individuals for reasons other than selection criteria</p> <ul style="list-style-type: none"> – “Ghost beneficiaries” – Registration of friends and family of staff <p>Exploitation: Inappropriate demands in exchange for registration (i.e. registration fees)</p>	<ul style="list-style-type: none"> • Organised beneficiary selection process that is structured to include checks and balances • Verification of beneficiary lists • Monitoring and evaluation conducted by independent, non-project staff • Community sensitisation on how beneficiaries are selected and that registration is free
Finance	<p>Delays in wire transfer to earn interest by staff at financial institution</p> <p>Unsolicited payments from transfer company, local partner, or financial institutions</p> <p>Corruption: Theft of project cash at any point before cash is received by beneficiaries</p>	<ul style="list-style-type: none"> • Ensure standardised timing for transfers • Scrutiny of extended or inconsistent transfer times • Strong internal controls and separation of responsibilities within the finance unit • Random, unannounced spot checks of financial records • Scrutiny of gaps in records or computer “crashes” in which data is lost
Operations – Logistics	<p>Bribes or unsolicited payments related to the sourcing of cash transfer mechanisms (i.e. in return for preferential treatment for one cell phone company versus another)</p>	<ul style="list-style-type: none"> • Ensure that procurement procedures are adhered to for financial institution or transfer company
Monitoring and Evaluation	<p>Fraud: Deliberate falsification of documents or manipulation of M&E processes to prevent the detection of fraud in the programme</p> <p>Fraud: Failure to implement SOPs on M&E to prevent the detection of fraud in the programme</p>	<ul style="list-style-type: none"> • Separation of M&E responsibilities from implementation staff • Close, on-going relationship with community to ensure that concerns come to the attention of NGO staff • Complaint mechanism in place, such as complaint boxes or a hotline, to provide a safe, anonymous way for the community to communicate with NGO management

Source: Cross, T. and Johnston A. (2011) *Cash Transfer Programming In Urban Emergencies. A Toolkit For Practitioners*. CaLP.

9. SAMPLE POST-DISTRIBUTION MONITORING (PDM) TOOLS

The Somalia Cash Consortium developed a number of PDM tools for cash and vouchers that can be adapted for e-transfers.

For cash:

http://www.cashlearning.org/downloads/Somalia%20CVMG/Monthly%20PDM%20Cash_CVMG_2011.pdf

Start **MONTHLY CASH POST DISTRIBUTION MONITORING FORM**
Questionnaire Number: []-M-[]- [] VER 6 120911

A: PERSONAL INFORMATION

A1 ID Number
A2 District
A3 Village
A4 NGO
A5 Date of interview: []/[]/[] / []/[]/[] A6 Gender of respondent (1= M, 2= F)
A7 Gender of the head of the hh (1= M, 2= F) A8 Size of hh
A9 Number of children in the hh < 5 years old A10 Targeting criteria for beneficiary
Codes for A10: 1 = Nutrition Centre Card, 2 = Pregnant / Lactating Mother, 3 = Women headed HH, 4 = IDP, 5 = Community Based Targeting, 6 = Other
A11 Hawala agent used
A12 Name of Enumerator
A13 Which best describes your household status?
Codes for A13:
1 = normally resident in this area, 2 = moved here due to drought, 3 = moved here due to conflict, 4 = moved here for other reasons
A14 What is your household's usual livelihood strategy (code) [] [] []
Codes for A14: 1 = pastoralist, 2 = agro-pastoralist, 3 = agriculture, 4 = urban, 5 = other

B: COLLECTION OF CASH

B1 How many hours did you take to travel to the cash distribution site? (code) [] [] []
B2 How long did you have to wait at the distribution site to get cash? (code) [] [] []
Codes for B1 & B2: 1 = <0.5 hours, 2 = 0.5 - 1 hour, 3 = 1 - 1.5 hours, 4 = 1.5 - 2 hours, 5 = 2 - 2.5 hours, 6 = >2.5 hours
B3 The length of time I spent travelling to collect cash was acceptable (code) [] [] []
B4 The frequency with which the cash is distributed suits my household's needs (code) [] [] []
B5 The transfer is sufficient to cover my household's basic food needs (code) [] [] []
B6 I would prefer food or food vouchers rather than cash (code) [] [] []
B7 I am aware of a complaints mechanism to report problems with the programme (code) [] [] []
B8 Traders have increased their prices as a result of the cash transfers (code) [] [] []
B9 Control over the cash has caused conflict within my household (code) [] [] []
B10 Other members of the community are jealous of me because of the cash transfer (code) [] [] []
Codes for B3 - B10: 1 = agree, 2 = no opinion, 3 = disagree, 4 = NA
B11 How much cash did you receive? [] [] [] USD B12 Was this the amount you expected? (1 = yes, 2 = no) [] []
B13 How long ago did you receive your last cash transfer? (code) [] [] []
Codes: 1 = <1 week, 2 = 1 - 2 weeks, 3 = 2 - 3 weeks, 4 = 3 - 4 weeks, 5 = > 4 weeks
B14 How much did you spend on transport to and from the distribution site? [] [] [] [] [] SoSh
B15 Did you have to pay anyone in order to receive your cash? (1 = yes, 2 = no) [] [] []
B16 Rank the ease with which you collected your cash (code) [] [] []
B17 Rank the level of security at the cash distribution site (code) [] [] []

C: USE OF CASH AND MARKET BEHAVIOUR

Indicate how much of the last month's cash transfer was used for each item (in Somali Shillings)

a. Food [] [] [] [] [] []	i. Transport [] [] [] [] [] []
b. Gift/Share [] [] [] [] [] []	j. Rent or shelter materials [] [] [] [] [] []
c. Livestock [] [] [] [] [] []	k. Agriculture inputs [] [] [] [] [] []
d. Business investment [] [] [] [] [] []	l. Household items [] [] [] [] [] []
e. Water [] [] [] [] [] []	m. Firewood [] [] [] [] [] []
f. Medical [] [] [] [] [] []	n. Clothes / shoes [] [] [] [] [] []
g. School Fees [] [] [] [] [] []	o. Saved / in hand [] [] [] [] [] []
h. Debt repayment [] [] [] [] [] []	p. Other [] [] [] [] [] []

C1 Where did you exchange your cash? (code) [] [] []
Codes for C1:
1 = Local Hawala, 2 = Local trader to whom you have a debt, 3 = Other trader, 4 = Exchange agent, 5 = Bank, 6 = Other
C2 What exchange rate did you get for the cash you received? 1 USD = [] [] [] [] [] [] / SS

END OF QUESTIONNAIRE

For vouchers:

http://www.cashlearning.org/downloads/Somalia%20CVMG/Monthly%20PDM%20Voucher_CVMG_2011.pdf

Start **VOUCHER MONTHLY POST DISTRIBUTION MONITORING FORM**
Questionnaire Number: []-M-[]- [] VER 6 160911

A: PERSONAL INFORMATION

A1 ID Number
A2 District
A3 Village
A4 GPS (for IDP camps) N: [] E: [] AS NGO
A5 Date of interview: []/[]/[] / []/[]/[] A7 Gender of respondent (1= M, 2= F)
A6 Gender of the head of the hh (1= M, 2= F) A8 Size of hh
A9 Number of children in the hh < 5 years old A10 Targeting criteria for beneficiary
Codes for A10: 1 = Nutrition Centre Card, 2 = Pregnant / Lactating Mother, 3 = Women headed HH, 4 = IDP, 5 = Community Based Targeting, 6 = Other
A11 Name of Enumerator
A12 Which best describes your household status?
Codes for A12:
1 = normally resident in this area, 2 = moved here due to drought, 3 = moved here due to conflict, 4 = moved here for other reasons
A13 What is your household's usual livelihood strategy (code) [] [] []
Codes for A13: 1 = pastoralist, 2 = agro-pastoralist, 3 = agriculture, 4 = urban, 5 = other
A14 Did you get any of the following in the last 4 weeks (tick):
a. Plainly Nut [] b. CSB-Oh-beans [] c. Rice-Oh-beans [] d. Food Voucher []
e. Cash or CPW [] f. Medicine [] g. Water or Water Voucher [] h. NFVoucher []

B: COLLECTION AND CONTROL OF VOUCHERS

B1 How many hours did you take to travel to the voucher distribution site? (code) [] [] []
B2 How long did you have to wait at the distribution site to get vouchers? (code) [] [] []
Codes for B1 & B2: 1 = <0.5 hours, 2 = 0.5 - 1 hour, 3 = 1 - 1.5 hours, 4 = 1.5 - 2 hours, 5 = 2 - 2.5 hours, 6 = >2.5 hours
Record the respondents views on the following statements B3-B10 using the codes below.
B3 The length of time I spent travelling to collect voucher was acceptable (code) [] [] []
B4 The frequency with which the vouchers are distributed suits my household's needs (code) [] [] []
B5 I would prefer food rather than vouchers (code) [] [] []
B6 I would prefer cash rather than vouchers (code) [] [] []
B7 I am aware of a complaints mechanism to report problems with the programme (code) [] [] []
B8 Control over the vouchers has caused conflict within my household (code) [] [] []
B9 The transfer allowed me to invite non-household members to come and eat at my household (code) [] [] []
B10 Other members of the community are jealous of me because I receive vouchers (code) [] [] []
Codes for B3 - B10: 1 = agree, 2 = no opinion, 3 = disagree, 4 = NA
B11 Did you get the amount of vouchers you expected? (1 = yes, 2 = no) [] [] []
B12 How long ago did you receive your last vouchers transfer? (code) [] [] []
Codes for B12: 1 = <1 week, 2 = 1 - 2 weeks, 3 = 2 - 3 weeks, 4 = 3 - 4 weeks, 5 = > 4 weeks
B13 How much did you spend on transport to and from the distribution site? [] [] [] [] [] SoSh

C: REDEMPTION OF VOUCHERS AND MARKET BEHAVIOUR

C1 Did you get the quantity of commodities you expected when you exchanged your vouchers? (1 = yes, 2 = no) [] [] []

C2 How much of the commodities did you receive in exchange for your voucher	Oil (l) [] [] [] [] [] []	CSB (kg) [] [] [] [] [] []	Sugar (kg) [] [] [] [] [] []	Rice (kg) [] [] [] [] [] []	Flour (kg) [] [] [] [] [] []	Pulses (kg) [] [] [] [] [] []
---	---------------------------------	----------------------------------	------------------------------------	-----------------------------------	------------------------------------	-------------------------------------

C3 How much do you consume in the household? [] [] [] [] [] [] []
C4 How much did you sell? [] [] [] [] [] [] []
C5 How much did you give away / share? [] [] [] [] [] [] []
C6 How much do you still have in stock? [] [] [] [] [] [] []
Codes for C7: 1 = Increased, 2 = No change, 3 = Decrease
C7 Traders have changed their prices as a result of the voucher scheme (code) [] [] []
C8 How long did you have to wait at the shop to redeem vouchers (code) [] [] []
Codes for C8: 1 = <1/2 hour, 2 = 1/2 - 1 hour, 3 = 1 - 2 hours, 4 = > 2 hours
C9 Did you sell the vouchers? Code: (1 = Yes, 2 = No) [] [] []
C10 If Yes to C9, how much did you sell for? [] [] [] [] [] [] SoSh
Record the respondents views on the following statements C11 - C17 using the codes below.
Codes for C11 - C17: 1 = agree, 2 = no opinion, 3 = disagree, 4 = NA
C11 The food I get in return for the vouchers is sufficient to cover my household's basic food needs (code) [] [] []
C12 There are sufficient traders to satisfy the needs of all people redeeming vouchers (code) [] [] []
C13 The trader always exchanges the voucher for the correct quantities of food (code) [] [] []
C14 The trader always treats me with respect when I go to exchange my voucher (code) [] [] []
C15 The trader's premises is located an acceptable distance from my house (code) [] [] []
C16 The food that I get in return for the voucher is of an acceptable quality (code) [] [] []
C17 The trader allows me or other beneficiaries to exchange the vouchers for cash (code) [] [] []
C18 If C17 = yes, how much cash did you get? [] [] [] [] [] [] SoSh

END OF QUESTIONNAIRE

10. BENEFICIARY NOTICE AND CONSENT (PLAIN LANGUAGE TEMPLATE)

Agreement on personal data

Case/identifying number:

Name of beneficiary:

Date:

Place:

How form will be explained

Name of person explaining form: _____

Role of person explaining form: (e.g. case officer/volunteer) _____

Explanation by person filling in form will be in _____ (language of explanation by person filling in form) and translated into _____ (language that explanation will be made in to beneficiary). _____

Explanation will be assisted by

1. Translation by trained interpreter or
2. Informal translation by _____
(record name of translator and relationship to beneficiary e.g. sister, priest)
3. Assistance by trusted part _____
(record name of translator and relationship to beneficiary e.g. sister, priest)

If you want to be part of the [insert name of programme] then we need to ask you some questions. We use what you tell us about yourself to organise how you get the [insert benefit in programme/cash payment]. There are rules about what we can do with what you tell us. What you tell us is called personal data. These are the rules.

1. We can only use your personal data to do the things that you agree today. We want to use your data to run the [insert name of programme]. We use your personal data to:

- get the [name of benefit in programme/cash payment] to you
- stop the money being stolen
- learn how to make the [insert name of programme] better
- [Optional: include other benefits from [insert name of agency]]

We can only keep your personal data as long as we need it to do these actions. If we want to do something different with your personal data then we must talk to you again.

2. The personal data that we will ask you to give us today is [insert categories of data e.g. name, cellphone number, the data itself may be recorded on a separate form but that must be filled in only after this consent is obtained.]

3. We do share your personal data with others so that you can get the [name of benefit in programme/cash payment]. We will share it with [insert name of service provider e.g. bank or mobile network] or other [insert providers details] to get the [name of benefit in programme/cash payment] to you. When we share your personal data with these others they must also obey these rules. They are not allowed to use your personal data to sell you things, just to give [name of benefit in programme/cash payment] to you. You can always ask us with whom we've shared your information.

(continued from page 79)

4. We try our best to look after your personal data so that no-one else can use it except for those with whom we share it. Everyone who gets your personal data from us must try their best to look after it.

5. There is a risk that someone else could get your personal data from us by doing wrong. [If there is a significant threat that a governmental or other entity might obtain the data with negative consequences beyond breach of data privacy for the beneficiary then the person filling in the form should explain the threat at this point. It is not recommended that the nature of the threat be recorded since that might trigger retaliation against the organisation collecting the data to facilitate payment.]

6. We might have to give your personal data to a government because of laws.

7. If you think that we or someone that we've shared your personal data with has got it wrong then you can tell us to make it right.

8. If some of your personal data changes you can get us to change it.

9. If you think that we or someone that we've shared your personal data with has broken the rules you can complain to us. [Insert contact details of person in country responsible for ensuring compliance with Code of Conduct.]

Recording agreement

Now that you have heard these rules about what we do with your personal data do you agree to give us your personal data?

Yes No

If yes, then indicate how the beneficiary agrees.

1. Signing a copy of this form.

Signature _____

2. Making a thumbprint or fingerprint on a copy of this form.

Fingerprint

3. Making a mark next to his or her name. Name and mark: _____

4. Other way (write how the beneficiary agreed): _____

If no, then explain to the beneficiary that there is another way to get the benefit and what it is, or if there is no other way then explain to the beneficiary that there is no other way.

Source: CaLP (2013) *Protecting Beneficiary Privacy: Principles and Operational Standards for the Secure Use of Personal Data in E-Transfer Programmes*.

11. DATA PROTECTION MODEL CLAUSES/Aid AGENCY AND E-TRANSFER SERVICE PROVIDER

Overview

The model clauses provide for the following:

- establishing that the aid agency (the Agency) is the data controller - the initiator of the request for data processing
- the e-transfer service provider is the “data processor”
- the e-transfer beneficiary who discloses their personal data to the Agency is the “data subject”
- that the “data processor” can only process the data for the purposes of the contract (which need to be express) and under the written instruction of the data controller
- that the data processor must not disclose the data to any third party or subcontract to any third party without the consent of the data controller, must have adequate internal information security standards to prevent unauthorised access, processing or disclosure of data
- agreement as to what happens to the data at the end of the contract
- limitations on the data processor’s use of data for marketing, profiling and other commercial uses not aligned with processing authorised by the Agency
- limitations on contact with the data subjects (beneficiaries) i.e. all contact with the beneficiaries shall be through the Agency, unless otherwise agreed between the Agency and the third party
- that the data processor shall ensure that its personnel and sub-contractors acting under the direct or indirect control of the data processor in performance of the data processor’s duties to the Agency contractually agree to:
 - Comply with non-disclosure obligations to procure the confidentiality of the data
 - Comply with relevant data processor policies such as Privacy Policy, Security Policy aimed at complying with the data processor’s duties to safeguard the data
 - Comply with obligations to maintain the quality of the data handled by the relevant personnel and sub-contractors including the accuracy of the data

The clauses represent a minimum standard but may be amended by the relevant Agency to accommodate (i) variations in terminology and naming conventions in the data protection laws applicable to the countries; or (ii) to adopt higher standards of data protection; or (iii) to accommodate specificities in the engagement between the particular Agency (Data Controller) and Data Processor.

It is important to note, that over and above the requirements of the ‘Principles and Operational Standards For The Secure Use Of Personal Data In Cash And E-Transfer Programmes’, data protection laws in several countries provide that even where a Data Processor causes a loss or unauthorised disclosure of Personal Data, it is the Agency, the Data Controller, who will be ultimately responsible for the breach. Hence the Data Controller may be civilly or criminally liable for data protection breaches occasioned by the Data Processor. The Agency has an interest, therefore in adopting measures additional to the agreement to procure the Data Processor’s technological and organisational compliance with the agreement such as auditing the Data Processor’s compliance with the agreement or periodic reporting by the Data Processor on the privacy and security policies and procedures implemented by the Data Processor.

(continued from page 81)

Model Clauses

The Model Clauses below are drafted so as to constitute a distinct agreement. The clauses may however be inserted into master/main agreements which govern other aspects of the relationship between Agency and Affiliate/Service Provider.

AGREEMENT

BETWEEN:

- (1) [Name of Agency], having its registered office at [...] (the “Data Controller”); and
- (2) [Name of Affiliate/ Service Provider], having its registered office at [...] (the “Data Processor”).

PURPOSE OF THIS AGREEMENT

- A. For the purpose of facilitating electronic cash transfers from the Data Controller to a beneficiary receiving the cash transfer, the Data Controller collects and processes Personal Data of such beneficiaries.
- B. The Data Controller has engaged the Data Processor to render the Services which incorporates processing beneficiary data on the Data Controllers’ behalf.
- C. The Data Controller is subject to laws, regulations and codes of conduct, principles and operational standards that place obligations on the Data Controller to respect the privacy and protect the Personal Data of beneficiaries in the processing of such data, whether independently or through appointed Data Processors.
- D. Accordingly, this agreement pertains to the protection of Personal Data accessed or otherwise received; and processed by the Data Processor on the Data Controller’s behalf in the course of rendering the Services.

IT IS AGREED:

1. DEFINITIONS AND INTERPRETATION

1.1 In this agreement:

Data Controller means, the Agency being the person who determines the purposes for which and the manner in which any Personal Data are, or are to be, processed.

Data Processor means the Affiliate/Service Provider, a person who processes Personal Data on behalf of the Data Controller over the course of rendering the Services.

Data Subject means the beneficiaries of electronic cash transfers facilitated by the Agency and persons to whom the Personal Data refers.

Personal Data means any personal information including identifying information such as the name, identification or passport number, mobile telephone number, email address, cash transaction details, of whatever nature, format or media that by whatever means, is provided to the Data Processor by the Data Controller, is accessed by the Data Processor on the authority of the Data Controller or is otherwise received by the Data Processor on the Data Controller’s behalf and includes transactional or other information associated with the Data Subject generated by the Data Processor in the course of providing the service to the Data Controller.

Processing in relation to Personal Data, includes the obtaining, recording or holding of such data or carrying out any operation or set of operations on the data, including organization, adaptation, or alteration; disclosure by transmission, dissemination, or otherwise; and alignment, combination, blocking, erasure, or destruction.

Schedule means the schedules annexed to and forming part of this agreement.

Services means the specific activities for which the Data Controller has engaged the Data Processor as set out in Schedule A [or clause [...] of main/ master agreement].

(continued from page 82)

2. DATA PROCESSING

2.1 The Data Processor agrees to process the Personal Data to which this agreement applies, and in particular the Data Processor agrees that it shall:

- a. process the Personal Data in accordance with the terms and conditions set out in this agreement and where the standards imposed by the data protection legislation regulating the Data Processor processing of the Personal Data are higher than those prescribed in this agreement, then in accordance with such legislation;
- b. process the Personal Data strictly in accordance with the purposes relevant to the Services in the manner specified from time to time by the Data Controller; and for no other purpose or in any other manner except with the express prior written consent of the Data Controller;
- c. implement appropriate technical and organisational measures to safeguard the Personal Data from unauthorised or unlawful processing or accidental loss, destruction or damage, having regard to the state of technological development and the cost of implementing any measures, such measures shall ensure a level of security appropriate to the harm that might result from unauthorised or unlawful processing or accidental loss, destruction or damage and to the nature of the Personal Data to be protected;
- d. regard the Personal Data as confidential data and not disclose such data to any person other than to employees, agents or sub-contractors to whom disclosure is necessary for the performance of the Service and subject to [...] below or except as may be required by any law or regulation affecting the Data Processor;
- e. implement technical and organisational measures to procure the confidentiality, privacy, integrity, availability, accuracy and security of the Personal Data including establishing organisational policies for employees, agents and sub-contractors aimed at complying with the Data Processor's duties to safeguard the Personal Data in accordance with this agreement;
- f. implement backup processes as agreed between the Data Controller and Data Processor to procure the availability of the Personal Data at all times and ensure that the Data Controller will have access to such backup of the Personal Data as is reasonably required by the Data Controller;
- g. ensure that any disclosure to an employee, agent or sub-contractor is subject to a binding legal obligation to comply with the obligations of the Data Processor under this agreement including compliance with relevant technical and organisational measures for the confidentiality, privacy, integrity, availability, accuracy and security of the Personal Data. For the avoidance of doubt, any agreement with an employee, agent or sub-contractor shall not relieve the Data Processor of its obligation to comply fully with this agreement, and the Data Processor shall remain fully responsible and liable for ensuring full compliance with this agreement;
- h. comply with any request from the Data Controller to amend, transfer or delete Personal Data; provide a copy of all or specified Personal Data held by it in a format and or a media reasonably specified by the Data Controller within reasonable timeframes as agreed between the parties [Agency to insert relevant time periods at its discretion];
- i. should the Data Processor receive any complaint, notice or communication which relates directly or indirectly to the processing of the Personal Data or to either party's compliance with applicable law, immediately notify the Data Controller and provide the Data Controller with full co-operation and assistance in relation to any complaints, notices or communications;
- j. promptly inform the Data Controller if any Personal Data is lost or destroyed or becomes damaged, corrupted or unusable and at the request of the Data Controller, restore such Personal Data at its own expense;

(continued from page 83)

- k. in the event of the exercise by Data Subjects of any rights in relation to their Personal Data, inform the Data Controller as soon as possible;
- l. assist the Data Controller with all data subject information requests which may be received from any Data Subject in relation to any Personal Data;
- m. not use the Personal Data of Data Subjects to contact, communicate or otherwise engage with the Data Subjects including transmission of any marketing or other commercial communications to the Data Subjects, except in accordance with the written consent of the Data Controller or to comply with a court order. For the avoidance of doubt, the Data Processor is not prohibited from contact, communication or engaging with the Data Subject in so far as this does not involve processing of Personal Data and the Data Processor procures that the promotion or offer of services is not in any manner associated to the Data Controller or the Data Controller's services;
- n. notify the Data Controller of the country(s) in which the Personal Data will be processed where such country(s) is not the country of the Data Processor's registered office;
- o. not process or transfer the Personal Data outside of the country of its registered office except with the express prior written consent of the Data Controller pursuant to a request in writing from the Data Processor to the Data Controller;
- p. permit and procure that its data processing facilities, procedures and documentation be submitted for scrutiny by the Data Controller or its authorised representatives, on request, in order to audit or otherwise ascertain compliance with the terms of this agreement;
- q. advise the Data Controller of any significant change in the risk of unauthorised or unlawful processing or accidental loss, destruction or damage of Personal Data; and
- r. report [in accordance with agreed reasonable timeframes] to the Data Controller on the steps it has taken to ensure compliance with clause 3.1. of this agreement.

3. WARRANTIES

3.1 The Data Processor warrants that:

- a. it will process the Personal Data in compliance with laws, enactments, regulations, orders, standards and other similar instruments applicable to the Data Processor; and in accordance with the terms and conditions of this agreement;
- b. in order to observe the rights of ownership and/or other proprietary or intellectual property rights of the Data Controller in the Personal Data, not copy, retain or process the Personal Data in any manner over the course of this agreement and upon expiration or termination of this agreement, except as required by law or in accordance this agreement.

4. INDEMNITY

4.1 The Data Processor agrees to indemnify and keep indemnified and defend at its expense the Data Controller against all costs, claims, damages or expenses incurred by the Data Controller or for which the Data Controller may become liable due to any failure by the Data Processor or its employees, subcontractors or agents to comply with the obligations under this agreement.

(continued from page 84)

5. APPOINTMENT OF SUB-CONTRACTORS AND AGENTS/ COMPLIANCE BY SUB-CONTRACTORS and AGENTS

5.1 The Data Processor may authorise a third party (sub-contractor or agent) to process the Data:

- a. subject to the terms of this agreement;
- b. subject to the Data Controller's prior written consent, the validity of the consent will be conditioned on the Data Processor supplying the Data Controller with full and accurate details of sub-contractors or agents; and
- c. provided the relevant sub-contractor's or agent's contract terminates automatically on the termination of this agreement for any reason.

6. TERMINATION

6.1 This agreement shall terminate automatically upon termination or expiry of the Data Processor's obligations in relation to the Services.

6.2 The Data Controller shall be entitled to terminate this Agreement forthwith by notice in writing to the Data Processor if:

- a. the Data Processor is in a material or persistent breach of this Agreement which, in the case of a breach capable of remedy, shall not have been remedied within [...] days from the date of receipt by the Data Processor of a notice from the Data Controller identifying the breach and requiring its remedy; or
- b. the Data Processor becomes insolvent, has a receiver, administrator, or administrative receiver appointed over the whole or any part of its assets, enters into any compound with creditors, or has an order made or resolution passed for it to be wound up (otherwise than in furtherance of a scheme for solvent amalgamation or reconstruction).

6.3 On termination of this agreement the Data Processor shall, in accordance with the direction of the Data Controller:

- deliver or destroy all Personal Data supplied by the Data Controller in its possession or under its control;
- instruct all its employees, agents and sub-contractors to, facilitate and ensure the delivery or destruction of the Personal Data including copies of the Personal Data in accordance with the Data Controller's direction.

7. GOVERNING LAW

7.1 This agreement will be governed by the laws of [...], and the parties submit to the exclusive jurisdiction of the Courts of [...] for all purposes connected with this agreement, including the enforcement of any order or judgment made under or in connection with it.

8. WAIVER

8.1 Failure by either party to exercise or enforce any rights available to that party or the giving of any forbearance, delay or indulgence shall not be construed as a waiver of that party's rights under this agreement.

9. INVALIDITY

9.1 If any term or provision of this agreement shall be held to be illegal or unenforceable in whole or in part under any enactment or rule of law such term or provision or part shall to that extent be deemed not to form part of this agreement but the enforceability of the remainder of this agreement shall not be affected provided however that if any term or provision or part of this agreement is severed as illegal or unenforceable, the parties shall seek to agree to modify this agreement to the extent necessary to render it lawful and enforceable and as nearly as possible to reflect the intentions of the parties embodied in this agreement including without limitation the illegal or unenforceable term or provision or part.

12. DATA PROTECTION PRINCIPLES

1 RESPECT

Principle: Organisations should respect the privacy of beneficiaries and recognise that obtaining and processing their personal data represents a potential threat to that privacy.

2 PROTECT BY DESIGN

Principle: Organisations should “protect by design” the personal data they obtain from beneficiaries either for their own use, or for use by third parties for each cash or e-transfer programme they initiate or implement.

3 UNDERSTAND DATA FLOWS AND RISKS

Principle: Organisations should analyse, document and understand the flow of beneficiary data for each cash or e-transfer programme they initiate or implement within their own organisation and between their organisation and others and develop risk mitigation strategies which might be required to address any risks arising from these flows;

4 QUALITY AND ACCURACY

Principle: Organisations should ensure the accuracy of the personal data they collect, store and use, including by keeping information up to date, relevant and not excessive in relation to the purpose for which they are processed, and by not keeping data for longer than is necessary.

5 OBTAIN CONSENT OR INFORM BENEFICIARIES AS TO THE USE OF THEIR DATA

Principle: At the point of data capture, beneficiaries should be informed as to the nature of the data being collected, who it will be shared with, who is responsible for the secure use of their data and be provided with the opportunity to question the use made of the data and withdraw from the programme should they not wish their personal data to be used for the purposes described.

6 SECURITY

Principle: Organisations should implement appropriate technical and operational security standards for each stage of the collection, use and transfer and use of beneficiary data to prevent unauthorised access, disclosure or loss and in particular any external threats should be identified and actions taken to mitigate any risks arising.

7 DISPOSAL

Principle: Organisations should not hold beneficiary data for longer than is required unless they have clear, justifiable and documented reasons for doing so otherwise data held by the organisation and any relevant third parties should be destroyed.

8 ACCOUNTABILITY

Principle: Organisations should establish a mechanism whereby a beneficiary can request information about what personal data an organisation holds about them, and mechanisms to receive and respond to any complaints or concerns beneficiaries may have about the use of their personal data.

Source: CaLP (2013) *Protecting Beneficiary Privacy: Principles and Operational Standards for the Secure Use of Personal Data in E-Transfer Programmes*.



The Cash Learning Partnership

Electronic transfers, or e-transfers, are a form of value transfer that relies on digital payment systems. The great many benefits they can realise for aid recipients and aid agencies alike in terms of increased security, convenience, privacy, speed, reduced operational/transaction costs and logistics, etc. have been widely documented. Equally, many aid agencies have experienced challenges in implementing e-transfers, including in relation to mobile network coverage and reliability, the presence of e-transfer agents, liquidity constraints and low education levels among beneficiaries. Learning from and responding to these challenges is essential.

These *E-transfers in Emergencies: Implementation Support Guidelines* are intended for the field practitioners of aid agencies engaged in humanitarian responses incorporating cash transfers to be delivered through digital payment systems as well as their extended teams in management and programme support functions.

These *E-transfers in Emergencies: Implementation Support Guidelines* assume prior knowledge of cash transfer programming and focus exclusively on implementing e-transfers and do not elaborate on decisions relating to whether or not cash is a viable programme option. Therefore, the programme lifecycle begins with assessing which e-transfer option is best suited to deliver a given cash-based intervention.

These *E-transfers in Emergencies: Implementation Support Guidelines* are designed as guidance sheets that can be used as reference documents to enable practitioners to easily access their sections of interest or relevance, yet some elements are cross-referenced throughout the documents.

The guidelines are organised into 5 sections:

- A. Types of e-transfer mechanisms
- B. Choosing e-transfer mechanisms
- C. Setting up and using e-transfer mechanisms
- D. Compliance, Monitoring and Evaluation, Data Protection and Complaints
- E. Additional guidance

Specific headings are used to guide the reader:

- “Key learning points” open each section, summarising the major learning of the section.
- “Key elements to consider” introduce the main issues discussed.
- “Example from the field” introduces case study boxes to give field-based illustrations of the issues discussed.
- “Additional guidance” introduces specific tools that can be found in Section E.

This research was commissioned by the Cash Learning Partnership (CaLP),
with the generous support of VISA Inc. and DFID

