E-transfers in Remote Emergency Programming

V0.1 July 2016

TABLE OF CONTENTS

[INTRODUCTION 2](#_Toc448996487)

[E-TRANSFER OPTIONS 2](#_Toc448996488)

[REMOTE PROGRAMMING PRINCIPLES 3](#_Toc448996489)

[REMOTE E-TRANSFERS MECHANISM SELECTION 4](#_Toc448996490)

This document covers humanitarian aid activities implemented with the financial assistance of the European Union. The views expressed herein should not be taken, in any way, to reflect the official opinion of the European Union, and the European Commission is not responsible for any use that may be made of the information it contains.

Comment and queries to [roger.dean@nrc.no](mailto:roger.dean@nrc.no)

INTRODUCTION

E-transfers are a digital replacement for paper vouchers or physical cash, and a disbursement mechanism rather than a specific type of Cash Transfer Programming (CTP). Remote programming is a range of operational models in which field access is restricted for senior managers for a sustained period of time. It is a system of last resort, although it is increasingly being used to allow entry to new humanitarian contexts.

*NRC’s Remote Cash Project guidelines* [bit.ly/1Tk9K6b](http://bit.ly/1Tk9K6b)

*Mercy Corps’ E-transfer Implementation Guide* [bit.ly/1UUMw6R](http://bit.ly/1UUMw6R)

When correctly selected for a remote emergency context, e-transfers can automate and increase efficiency of cash transfer programmes. However the increased risks and constraints associated with remote programming mean that good mechanism decision-making is essential.

## HOW TO USE THIS GUIDE

This document is an annex to both the Norwegian Refugee Council (NRC) Remote Cash Project guidelines and the Mercy Corps E-transfer Implementation Guide.

If you are using the Remote Cash Project guidelines, you will need this document at the Delivery Mechanism Selection part of Section 2.

If you are using the E-transfer Implementation Guide (and the accompanying Cash Transfer Programming Methodology Guide), this document will be most useful for the Feasibility Assessment section.

This document will focus on e-cash (cash replaced with mobile money, ATM/debit cards etc.) and e-vouchers (replacements for paper vouchers).

E-TRANSFER OPTIONS

E-cash options allow a project participant to access currency from a cash-out point. They include –

* Regular bank debit or credit cards, or account-free prepaid cards, usable at suitable equipped shops and ATMs
* Mobile phone-based systems where cash can be withdrawn from associated banks, shops or other facilities

E-vouchers are electronic versions of ‘closed loop’ voucher systems, in which vendors are typically reimbursed for their goods or services outside of the e-voucher system. They include -

* Smart card e-vouchers, such as those offered by [Red Rose](https://www.redrosecps.com/), [sQuid](https://www.squidcard.com/) and [MasterCard](https://youtu.be/W2XIyqeP5w4)
* Smartphone e-vouchers, such as those offered by [Transversal](http://www.transversal.ht/mobi.html)

The marketplace for these services is changing fast, and there may also be providers based in the country of operation – these should be given due consideration, with local development benefits taken into account.

E-transfers can add value to a project by –

* Saving project participants’ time and reducing risks – entitlements can be delivered remotely so repeat distributions are not necessary
* Giving project participants privacy – low-profile deliveries can reduce the risk of theft, ‘taxation’ or coerced sharing from authorities or others
* Giving better data – automated usage and market monitoring data cuts monitoring time and costs and greatly improves agencies’ decision-making, support and audit capacities
* Offering vendors and agencies quicker and easier reconciliation than with paper vouchers

Potential downsides include –

* Technology barriers – PINs, passwords and mobile phone based systems can be difficult for participants with limited exposure to technology. Importation of technology can be time-consuming, especially in sanctioned countries.
* Privacy and protection – service providers’ Know Your Customer (KYC) requirements could make peoples’ status as project participants, location and phone number known to a government. Weak data protection can result in wider ‘leaks’. People without adequate ID may not be able to enrol for the service at all
* Liquidity – large scale e-transfers (or any system with a cash-out facility) may outstrip transfer agents’ capacity
* Reliability of service – the quality and reliability of service providers varies considerably and can be difficult to assess in advance
* Slow startup – setting up e-transfers takes longer. Even in a ‘normal’ operating environment it can take several months from programme start to getting the first payments out

REMOTE PROGRAMMING PRINCIPLES

A recap of the themes of remote programming. The key ones for e-transfers in remote emergencies will be explored below:

* Plan for it
* Prioritise professional development support for field staff and/or partners
* Consider the ethical implications of risk transfer to field staff and/or partners
* Decrease project complexity
* Adapt structures and procedures
* Make additional and regular checks on procedures and resources
* Prioritise honest and well-documented communications with staff/partners, stakeholders and donors

## PLANNING

The emphasis on planning and preparedness is common to both remote cash programming in general and e-transfers in particular. When contemplating doing both, agencies and donors need to have realistic expectations. It may be that an alternate modality or delivery mechanism is required to meet immediate needs until an e-transfer system can be established. This alternate modality may need to be retained as a contingency plan in case of sudden changes in operating environment.

## REMOTE STAFF / PARTER CAPACITY

A wide range of technical support functions will need to be performed by remote staff/partners. Project participants will need training and troubleshooting support for unfamiliar hardware and software. Vendors will need monitoring and may need support as they operate Point of Sale equipment. This is all in addition to the ‘programming’ tasks required to deliver the sectoral or multi-sectoral outcomes required – agencies must make sure the necessary awareness-raising and programming activities are still done well.

The competence and speed with which remote staff or partners can respond to needs arising from project participants technology barriers may be crucial to the smooth running of an e-transfer project. Solutions using PIN numbers are most common, and yet PIN numbers can be very difficult for people who have not used them before. System-building in advance for replacing forgotten PIN numbers is important. If a more flexible solution is possible, a participant-chosen ‘secret password’ may have fewer problems. Find ways to test your problem-solving solutions as part of the remote staff or partner training routines.

## REDUCING PROJECT COMPLEXITY

The introduction of e-transfers can reduce complexity in labour-intensive areas such as recurring distributions, usage monitoring and vendor reconciliation, areas with which local staff/partners may be relatively familiar. Meanwhile complexity is increased in some more technically specialised areas such as providing technical support and troubleshooting for project participants and vendors. Solutions to problems may take longer to be understood and communicated and a different and more specialised skillset may be required for staff/partners, potentially including IT, case management data processing, and context-specific adult learning techniques.

REMOTE E-TRANSFERS MECHANISM SELECTION

## FEASIBILITY

Prior to assessing e-transfer feasibility, it will have been decided whether a cash or a voucher modality better suits the needs and project objectives. The conditions in the programme area may then force a re-think, as e-cash generally needs better network connectivity and security conditions to enable clash out.

The feasibility of e-transfers in a remote emergency context rests largely on service provider capacity, and that depends on the reliability of key infrastructure such as banks, electricity, mobile phone and internet connectivity. This infrastructure may be more resilient in contexts where cyclical natural hazards (e.g. floods in Bangladesh) are the reason for a remote programming approach. In complex emergencies (e.g. war in Syria) the functionality of infrastructure may be part of the conflict dynamic, with reliability and safe usage more limited.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Reason for remote approach | Likely banking functionality | Likely electricity availability | Likely mobile phone functionality | Likely internet connectivity | Possible e-transfer systems |
| Cyclical natural hazard prevents access (e.g. seasonal floods) | Unchanged | Reduced | Unchanged | Unchanged | Any |
| Sudden impact natural hazard prevents access (e.g. tsunami) | None | None | Reduced | Reduced | Smart card e-vouchers, mobile money |
| Low level insurgency / terrorism (government holds all territory) | Unchanged, but increased scrutiny | Unchanged | Unchanged, but increased scrutiny | Unchanged, but increased scrutiny | Any |
| Open conflict – government area (relatively static lines of control) | Unchanged | Unchanged | Unchanged | Unchanged | Any |
| Open conflict – opposition area (relatively static lines of control) | None | Reduced | Reduced | Reduced | Smart card e-vouchers, mobile money |
| Open conflict – government area (highly changeable lines of control) | Reduced | Reduced | Reduced | Reduced | All options possible but unreliable. Perhaps unsuitable for e-transfers |
| Open conflict – opposition area (highly changeable lines of control) | None | None | None | None | Unsuitable for e-transfers |

## ACCESSIBILITY

Project participants’ and vendors’ familiarity with e-transfer technology can be a barrier in any such project. In a remotely managed project much of the technical support and troubleshooting role will be carried out by remote staff/partners, who may themselves need additional time and support. Mechanisms which require PIN numbers are often particularly challenging, with a high error rate among project participants compounded by potentially lengthy processes to issue new codes in a remote emergency.

A more important determinant of project success though is participants’ access to vendors or cash-out facilities where they can use their e-transfers. In non-remote contexts this is usually mostly down to distance, but in a remote emergency factors such as safety to travel, checkpoints, and the physical condition of roads and bridges will be key. Make sure participants feel they can get to vendors and cash-out facilities easily, safely and at a reasonable cost. Make sure the differing needs of women and men, elderly and disabled people, and people of different perceived affiliations are understood.

## DATA PROTECTION

Project participants’ data is only as secure as the weakest link in the programme chain, from collection all the way through to retention or disposal. A data flow mapping exercise, ideally before data collection starts, can be useful to identify points of weakness and eliminate unnecessary steps. Including remote staff and/or partners in this will also increase awareness and should be part of training plans.

*ELAN’s Data Starter Kit gives simple, practical tip sheets on data in e-transfers* bit.ly/259mYp8

E-cash service providers must adhere to national financial regulations, typically including Know Your Customer requirements. KYC regulations are designed to counter threats to the financial system, including money laundering and terrorist financing. Service providers must collect and give authorities access to varying levels of information about project participants. In conflict environments (as many remote emergencies are) governments are more than usually interested in where people are and what resources, especially cash, they have access to.

Project planners should take a cautious approach to e-cash mechanisms in contexts where participants could be at risk from their own governments. E-vouchers do not require KYC on the part of the service providers (although agencies are still required to justify their project participant selection, and carry out due diligence on vendors) and may be a better choice in such situations.

The increasing use of cloud-based tools to gather and store personally identifying information is a significant issue to be considered in a mapping exercise, but typically the biggest data protection gains can be made by tightening office-level controls on spreadsheets and paper files.

When planning assessments and monitoring, make sure the data to be collected is only what is required and does not put people at risk or breach privacy. Be aware of the requirements of national data protection laws.