NORWEGIAN REFUGEE COUNCIL

REFERENCE GUIDE

HUMANITARIAN ORGANISATIONS' USE OF MONEY SERVICE PROVIDERS

Funded by
the European Union

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Foreign Affairs FDFA

NRC

NORWEGIAN
REFUGEE COUNCIL

ACKNOWLEDGEMENTS

The Norwegian Refugee Council (NRC) is an independent, international, humanitarian non-governmental organisation (NGO) that provides assistance and protection and contributes to durable solutions for refugees and internally displaced people worldwide.

NRC produced this report with financial assistance from the European Union's Directorate-General for European Civil Protection and Humanitarian Aid Operations and the Swiss Federal Department of Foreign Affairs (FDFA).

The report was researched and written by Paul Hausmann. It benefits from the invaluable contributions of key informant interviewees from various NGOs, international organisations, banks, money service providers and donor governments. NRC would like to thank those who contributed their time and expertise to this work.

For further information, please contact nrcgeneva.policy@nrc.no

Cover photo: Woman in Renk Transit Centre, South Sudan. © Richard Ashton/NRC

Editor: Jeremy Lennard

Layout & Design: BakOS DESIGN

TABLE OF CONTENTS

TERMS AND DEFINITIONS

Aid diversion: Any event, including fraud, corruption, bribery, theft, money laundering and other misuse of funds, that prevents funds being directed to its intended recipients.[1]

Counterterrorism measures: International, regional and national laws and policies or donor provisions related to counterterrorism. They include sanctions adopted for counterterrorism purposes and criminal laws.

Derisking: When the private sector or financial institutions terminate or restrict financial services to avoid rather than manage risk. Bank derisking is driven by risk aversion, concerns about reputation and profitability, and requirements to comply with sanctions, anti-money laundering (AML) and countering the financing of terrorism (CFT) obligations.

Due diligence: The application of organisational policies, controls and processes designed to identify and assess the impact of activities and relationships on humanitarian work throughout the project cycle.

Humanitarian safeguard or carve-out: Non-legal terms that refer to approaches taken to exempt organisations or activities from restrictions that legal provisions impose to protect principled humanitarian action. As far as sanctions are concerned, there are two main approaches: safeguards that apply automatically, often referred to as exemptions or general licenses; and safeguards for which organisations have to apply for on a one-off basis, often referred to as derogations and specific licenses.

Hawala: A non-bank financial service characterised by the settlement of imbalances through trade, cash and/or long-term net settlement rather than a simultaneous wire transfer.

Know your customer/supplier: A due diligence measure to verify the identity of a customer/supplier which involves the collection of information, including name, address and copy of government-issued ID.

Money laundering: The process of concealing the origins of money obtained from illicit activities and making it appear to have come from a legitimate source.

Money service provider: A non-bank financial service provider that makes money available to third parties in other geographical locations. They can be formal or informal entities.

Sanctions: Foreign policy measures that may be adopted internationally or by regional organisations and/or individual countries. They are intended to influence the behaviour of other countries, groups or individuals without recourse to armed force. They may include financial sanctions, prohibitions on the purchase of commodities or the import of certain goods, and travel restrictions for designated individuals.

[1] This is NRC's internal definition of aid diversion. Other definitions exist in the humanitarian sector, including those that distinguish between fraud and diversion. ECHO, for instance, defines aid diversion as an event that "occurs when, due to the action or inaction of actor/s external to DG ECHO's partner, its staff or its implementing partner(s), aid is prevented from reaching the action's intended beneficiaries or activities".

EXECUTIVE SUMMARY

This paper provides an overview of how humanitarian organisations use money service providers (MSPs) to enable their operations. It is intended to consolidate and improve the knowledge of all stakeholders involved in the topic, including on terminology, legal frameworks, donor positions and policies, reasons for using MSPs and the risks associated with doing so. It also sets out the steps humanitarian organisations take to ensure they use MSPs safely and responsibly. To achieve this, the report builds on desk research and key informant interviews with more than 20 experts from humanitarian organisations, banks, donor governments and MSPs.

WHAT ARE MSPS AND HOW ARE THEY REGULATED?

In settings disconnected from the international banking system or suffering liquidity constraints, humanitarian organisations often have to rely on MSPs to transfer and receive funds. The humanitarian community describes MSPs in a number of ways, but for the purpose of this paper the term is used to refer to non-bank financial service providers that make money available in another geographical location.

There is no global regulatory framework for MSPs and requirements vary by country. The Financial Action Task Force (FATF) has, however, provided global recommendations to states for MSPs' regulation to address money laundering and financing of terrorism risks. UN Security Council (UNSC) resolution 2462 also requires states to consider the potential effects of these measures on humanitarian activities.

HOW DO HUMANITARIAN ORGANISATIONS USE MSPS?

Humanitarian organisations increasingly use MSPs for cross-border payments because of bank derisking and the decrease in correspondent banking networks. They have become a vital means of reaching people in need of aid in some areas. Organisations mostly use MSPs registered with competent authorities, but this is not possible in all humanitarian settings. In areas outside central government control and where regulatory systems for MSPs are lacking, they may have to rely on unregistered providers, in which case additional due diligence measures may be triggered to manage associated risks.

WHAT ARE DONORS' POSITIONS ON THE USE OF MSPS?

Donor agencies and governments widely acknowledge the vital role of MSPs in supporting humanitarian operations, particularly where traditional banking services are limited or unavailable. The EU's Directorate-General for European Civil Protection and Humanitarian Aid Operations (ECHO) has issued the most comprehensive guidance on the use of MSPs, which reaffirms their important role in humanitarian responses.

WHAT RISKS ARE ASSOCIATED WITH THE USE OF MSPS?

Donors and humanitarian organisations emphasise the importance of adopting a holistic approach to assessing risks associated with the use of MSPs, including the inadvertent violation of sanctions or anti-money laundering (AML) and countering the financing of terrorism (CFT) legislation but also the potentially severe consequences of not using MSPs in the absence of alternatives, which can delay or entirely prevent the provision of humanitarian assistance. Organisations and states work hard to manage such risks and share the objective of ensuring that all aid reaches its intended beneficiaries, but they also understand that it is not always possible to eliminate all risks entirely.

The Financial Action Task Force Recommendations set out a comprehensive framework of measures which countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction. The FATF Recommendations relating to MSPs requires states to license MSPs and ensure adequate and

relevant regulation. At the same time, UNSC Resolution 2462 requires States to consider the potential effects of these measures on humanitarian activities.

GOOD PRACTICE IN THE USE OF MSPS

The second half of this paper sets out examples of good practice, including risk mitigation measures, which humanitarian organisations have developed over years of working with MSPs:

- **Use of registered and regulated MSPs:** Organisations use registered MSPs whenever possible to ensure legal compliance and mitigate risks. Exceptions if registered providers are unavailable, particularly in high-risk areas, allow them the flexibility required to ensure continuity in their operations.

- **Know your supplier (KYS) procedures:** Beyond standard procurement policies, organisations may adopt specific KYS procedures to verify MSPs' identities. These include checking registration documents and bank details, identifying owners and conducting site visits. They also gather references, especially from NGOs and UN agencies, and verify licenses to assess associated risks.

- **Sanctions and counterterrorism measures:** Organisations incorporate sanctions and counterterrorism screening into procurement policies for MSPs.

- **Payment in arrears:** Organisations typically pay MSPs in arrears. This minimises risks, especially with new or unlicensed providers. Advance payments are generally only made in emergency situations when other options are unavailable, and when the organisation has a trusted relationship with the MSP in question.

- **Diversifying engagement with MSPs:** Organisations often sign framework agreements with various MSPs, which allow for swift shifts to alternative providers during crises.

Internally displaced persons forced to flee North Kivu province, DRC. © Beate Simarud/NRC

- **Community-informed MSP selection and post distribution monitoring:** When using MSPs for cash-based assistance, organisations often consult local communities to select trusted providers. They also manage aid diversion risks by obtaining confirmation of receipt from beneficiaries before reimbursing MSPs.

- **Trust building with donors and banks:** Some organisations proactively share information with donors and banks on their use of MSPs. This has led some donors to support them with written approval letters to use certain MSPs and banks' willingness to process transfers to MSPs.

- **Knowledge sharing on MSPs:** Organisations regularly participate forums such as cash working groups to share knowledge on MSPs' reliability, commission rates, regulatory requirements and operational challenges.

The paper concludes with 10 recommendations each for organisations and donors to promote the safe, reliable and efficient use of MSPs in humanitarian operations.

1 INTRODUCTION

One of the biggest operational challenges humanitarian organisations face is their limited access to financial services as a result of bank derisking. This occurs when banks refuse to offer services, such as opening accounts or processing transfers, to organisations or locations perceived as high-risk to avoid falling foul of sanctions and anti-money laundering (AML) and countering the financing of terrorism (CTF) measures, which may have criminal, financial and reputational consequences.

Derisking has increased over the past decade in response to the proliferation of sanctions and counterterrorism (CT) measures, and this has reduced the number of formal banking channels available to humanitarian organisations for the transfer of funds to the countries in which they operate. In settings that are largely or entirely disconnected from the international banking system or suffering serious liquidity constraints, organisations often rely instead on money service providers (MSPs).[2]

Recognising the importance of MSPs in humanitarian action, NRC held an expert workshop in December 2022 which explored their use and related challenges, and made corresponding policy recommendations.[3] Most of the donors who participated emphasised the important role that MSPs play. They also acknowledged associated risks, but it was banks that were most concerned about the latter.

Participants also recognised a lack of awareness across stakeholders on what MSPs are, the difference between regulated and unregulated providers, and how humanitarian organisations use MSPs, including common commission rates, coordination and information exchange and risk mitigation measures. To address these knowledge gaps, NRC has developed this reference guide based on 20 key informant interviews with experts from humanitarian organisations, banks, donor governments and MSPs.

Staff with diverse technical backgrounds were interviewed, including finance, legal, grant management, cash and voucher assistance (CVA) and market analysis specialists. The document captures the knowledge organisations have developed over years of working with MSPs and provides a detailed overview for those not regularly exposed to the topic. This is intended to support humanitarian work while also promoting donors' and banks' understanding of the risk mitigation measures taken when working with MSPs.

The guide is written for generalists without technical knowledge of MSPs and those more experienced with the topic.

---

2 NRC, Safeguarding Humanitarian Banking Channels: How, Why and by Whom? January 2023.

3 More information on NRC's multistakeholder dialogue series on solutions to derisking can be found here; the findings of the session on MVTS are summarised here.

2 BACKGROUND

2.1 TERMINOLOGY AND LEGAL FRAMEWORK

2.1.1 DEFINING MSPS

Various terms are used to refer to non-bank financial service providers, including *hawala*, money transfer agents, money service businesses, cash agents, informal financial service providers and MSPs. Some are used colloquially, while others are legal terms used in certain jurisdictions to refer to licensed non-bank financial service providers.[4]

The Financial Action Task Force (FATF),[5] the main intergovernmental body tasked with setting standards to limit money laundering and terrorism financing, uses the term money or value transfer service (MVTS) when referring to registered non-bank financial service providers.[6] Depending on the region in which the transaction is processed, MVTS providers may be referred to using specific terms, including *hawala, hundi* and *fei-chen*.[7]

The FATF classifies hawala as a subset of MVTS, provided they are registered with the appropriate authorities. It does not consider large multinational money transfer networks, such as Western Union and MoneyGram, or new payment methods such as mobile money remittance services that humanitarian organisations use in CVA programming, as hawala.[8] It views them instead as different types of MVTS.[9]

This paper uses the term MSP to refer to non-bank financial service providers that make money available in another geographical location, including those providers operating informally. This is crucial to capture the wide range of non-bank financial service providers humanitarian organisations must rely on to sustain their operations. It is also more neutral and inclusive of the different types of providers used than the commonly used term hawala, which is associated with unregulated providers in some countries and sectors. One donor interviewed for this paper confirmed that for these reasons it had also adopted different terminology.

Figure 1 illustrates the money flow and parties involved in a basic transaction through an MSP, with MSP 1 representing the party to which an organisation sends money to be transferred cross-border and MSP 2 the party paying the equivalent to the recipient in the country of operations. Transactions may involve one or several intermediaries and a final payment to a third party.

---

4 HMRC, Money service business guidance for money laundering supervision, 8 February 2024; US Treasury, Money Services Business Definition, undated.

5 The FATF is the main intergovernmental body tasked with setting standards to limit money laundering and terrorist financing risks. Its guidance is not legally binding, but it carries significant weight because it carries out regular evaluations of countries' compliance with its standards. In case of non-compliance, it may add a country to its grey or blacklist, which may impede that country's access to the international financial system. The FATF's central role in combatting money laundering and terrorism financing is reaffirmed in UN Security Council resolution 2462.

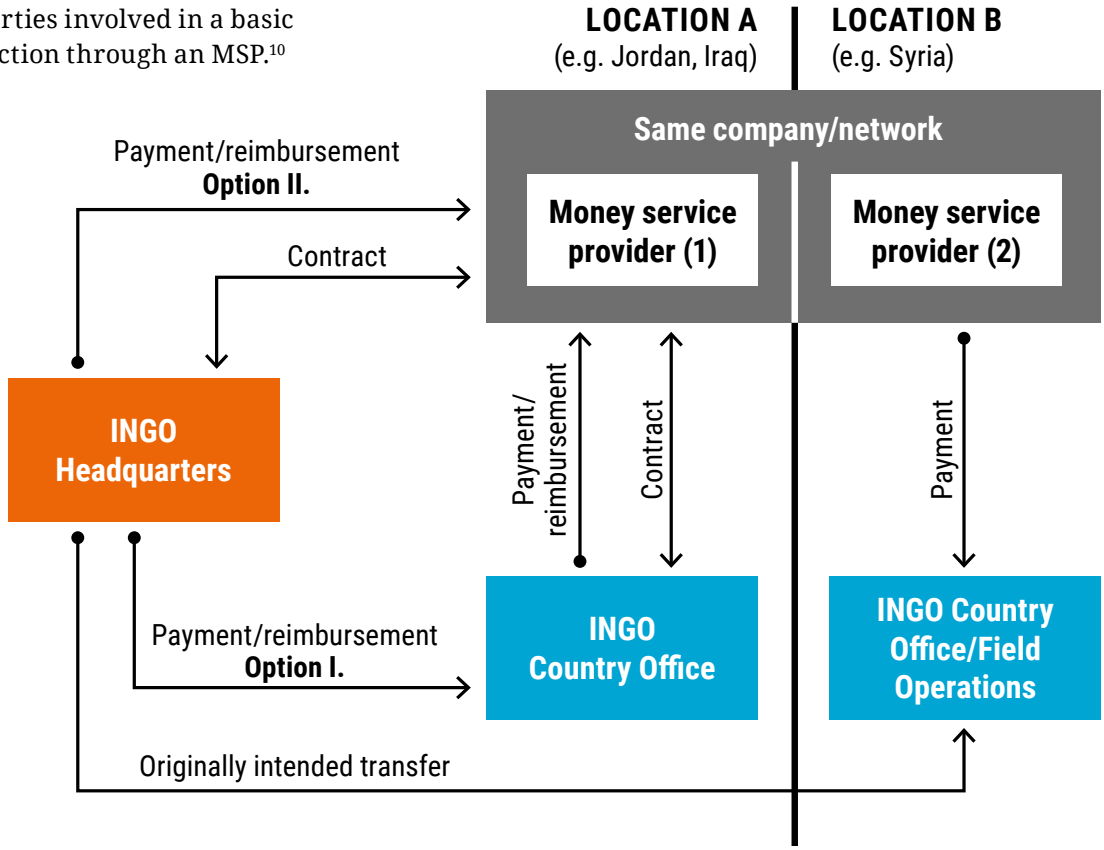
6 The FATF's definition of an MTVS can be found here.

7 FATF, Guidance for a Risk-Based Approach for Money or Value Transfer Services, 2016.

8 *Hawala* providers are distinguished by their connections to specific geographical regions or ethnic communities and by settling balances through trade, cash or long-term net settlements, rather than immediate wire transfers.

9 FATF, The role of hawala and other similar service providers in money laundering and terrorist financing, October 2013.

Figure 1: Overview of money flow and parties involved in a basic transaction through an MSP.[10]



KEY TAKEAWAYS

- **Different terms:** The humanitarian community uses various terms, such as *hawala*, money service businesses and MSPs, to describe non-bank financial service providers.
- **FATF definition:** The FATF classifies these providers as MVTSs and requires countries to license or register them with the competent national authorities.
- **Paper's working definition:** The paper adopts the term MSP to encompass both registered and informal non-bank financial service providers, reflecting the diverse types of provider humanitarian organisations use for financial transactions.

2.1.2 LEGAL FRAMEWORKS REGULATING THE USE OF MSPS

Global legal frameworks

There is a common misconception that the MSPs humanitarian organisations use by definition operate informally, when in fact many are formally registered as financial service providers with competent national authorities.[11] This misconception is aggravated by the use of the term hawala, which is often taken as synonymous with informality. When organisations say they use hawala services, it may be perceived in some countries as admitting to unlawful behaviour, when in reality the MSPs used are registered.

There is no global regulatory framework for MSPs. Domestic regulation and licensing requirements differ between countries. The FATF

[10] Schramm M and Taube M, The institutional foundations of al qaida's global financial system, undated.

[11] This can be illustrated by examining how differently the regulatory bodies of the UK and Germany communicate on this matter. Germany's Federal Financial Supervisory Authority (BaFin) states that *hawala* banking is illegal because by definition it fails to meet KYC standards in line with AML regulations, so the authority will not grant licences for hawala businesses to provide financial services. The UK Office of Financial Sanctions Implementation (OFSI) states that *hawala* banking is not illegal, but that providers must comply with the domestic rules and regulations for financial service providers. As such, there is no significant difference in the types of financial services that both regulators permit, but there is a difference in their definition of *hawala* banking.

Recommendations set out a comprehensive framework of measures which countries should implement in order to combat money laundering and terrorist financing, as well as the financing of proliferation of weapons of mass destruction. The FATF Recommendation 14 relating to MSPs, requires States to license MSPs and ensure adequate regulation and supervision. This regulation and supervision should be based on the assessed ML/TF risks to the sector. It states that:

"Countries should take measures to ensure that natural or legal persons that provide money or value transfer services (MVTS) are licensed or registered, and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations. Countries should take action to identify natural or legal persons that carry out MVTS without a license or registration, and to apply appropriate sanctions. Any natural or legal person working as an agent should also be licensed or registered by a competent authority, or the MVTS provider should maintain a current list of its agents accessible by competent authorities in the countries in which the MVTS provider and its agents operate. Countries should take measures to ensure that MVTS providers that use agents include them in their AML/CFT programmes and monitor them for compliance with these programmes."[12]

States also have obligations under UN Security Council (UNSC) resolution 2462, which urges them when designing and applying CT measures "to take into account the potential effects of those measures on exclusively humanitarian activities … that are carried out by impartial humanitarian actors in a manner consistent with international humanitarian law".[13] This means states should carefully consider the impact of any restrictions on humanitarians' use of MSPs and in turn their ability to provide assistance in settings where MSPs are a vital tool.

Regional and national legal frameworks

In the EU, so-called payment service providers must obtain a licence from member states to operate.[14] The licensing process includes a requirement to submit detailed information, including on internal control mechanisms established to comply with the EU's AML and CFT legislation. Humanitarian organisations are not allowed to use MSPs that do not fulfil these requirements in the EU.

Many of the countries where humanitarian operations take place have developed and improved their own domestic regulatory frameworks for MSPs in the last decade, including AML and CFT measures, to comply with FATF recommendation 14 on MVTSs.[15]

In Jordan, for example, the provision of non-bank financial services is regulated by the money exchange business law of 2015, which requires MSPs to obtain a license from the country's central bank before providing services.[16] Article 17 of the law states that MVTS providers must comply with Jordanian AML and CFT regulations, and article 21 that they must keep invoices and records of outgoing payments, prepare final financial statements and provide customers with copies of invoices. As a result, the FATF's 2019 mutual evaluation report found that Jordan was largely compliant with recommendation 14.[17]

Oraganisations interviewed for this paper were informed of domestic legal requirements in their countries of operation to ensure legal compliance, including by requesting licenses from potential MSPs before signing a contract.

---

12 FATF, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF recommendations, November 2023, p.17.

13 UNSC, Resolution 2462, 28 March 2019.

14 EU, Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, November 2015.

15 More information on the domestic regulation of MVTSs in specific countries can be obtained from the FATF's mutual evaluation reports.

16 FATF, The Hashemite Kingdome of Jordan Mutual Evaluation Report, November 2019; Government of Jordan, The Money Exchange Business Law, 2015.

17 Government of Jordan, The Money Exchange Business Law, 2015.

Bombed building in Kharkiv oblast, Ukraine. © Beate Simarud/NRC

Jurisdictions lacking a financial supervisory authority

Some jurisdictions or geographical areas lack a financial supervisory authority or are not under the control of the central government, meaning that licensing MSPs and enforcing AML and CFT rules may not be possible. These include the opposition-controlled parts of Myanmar, parts of eastern Democratic Republic of the Congo, Darfur and other areas of Sudan.

Governments are entitled under international law to adopt and enforce domestic financial policies that apply across their countries as a whole, but they tend not to issue licenses to MSPs operating in territory under the control of non-state armed groups. It follows that humanitarian organisations providing assistance in such areas may need to work with unlicensed MSPs.

In other countries experiencing internal conflicts with different fractions competing for control, separate regulatory structures have emerged. In Yemen, for example, Ansar Allah, also know as the Houthi movement, has set up its own central bank and introduced its own currency in opposition to the internationally recognised government in the south.[18] This may create competing legal obligations for humanitarian organisations using MSPs in such locations, particularly in areas where more than one party exerts an element of control.

Most donors acknowledge this operational reality and permit organisations to use MSPs which do not have a central government licence. For cross-boarder payments at least, registration is usually possible in the location where an organisation pays the provider through bank transfer.

[18] Associated Press, Fight for control of Yemen's banks between rebels, government threatens to further wreck economy, 16 June 2024.

KEY TAKEAWAYS

- **Misconceptions about MSPs:** There is a prevalent misconception that the MSPs humanitarian organisations use, particularly hawala, are inherently informal and unregulated. Most, however, are registered with national regulatory bodies that enforce corresponding obligations.
- **Diverse regulatory frameworks:** There is no global regulatory framework for MSPs, and requirements vary by country. The FATF in its global recommendations requires states to license MSPs and ensure adequate regulation and supervision.
- **UNSC resolution 2462:** The resolution urges states to take the potential effects of CT measures on humanitarian activities into account. This may include MSPs, particularly in settings where they are a vital tool for sustaining operations.
- **Licensing constraints in humanitarian settings:** Humanitarian organisations try to use registered MSPs, but this is not always possible. In areas outside central government control and/or without a regulatory system for MSPs, they may have to rely on unregistered providers.

2.2 WHY AND HOW DO HUMANITARIAN ORGANISATIONS USE MSPS?

Humanitarian organisations need to move funds to the areas where they operate to sustain their programmes. They aim to use the cheapest, fastest and safest providers available to maximise the assistance reaching beneficiaries, guarantee swift project implementation and minimise legal, reputational and operational risks. The traditional banking sector is the default conduit for such funds.

Organisations may, however, need to rely on MSPs to reach locations not serviced by the banking sector due to derisking, if the banking system has collapsed or lacks liquidity or if governments have imposed restrictions on access to financial services. That said, one donor noted that MSPs are not only used because banks are unavailable, but because sometimes they are the most reliable financial service provider available.

Humanitarian organisations use MSPs in two ways:

1. For cross-border payments to countries where they operate when correspondent banking networks are unavailable or difficult to use.[19]
2. For in-country transfers to pay salaries and suppliers or implement CVA programmes in remote areas.

The Middle East and North Africa was repeatedly mentioned the region where humanitarian operations are most reliant on MSPs, particularly Syria. Those in other countries, however, including Afghanistan, Burkina Faso, Democratic Republic of the Congo, Myanmar, Sudan and Ukraine, also rely on them. As derisking persists and some areas where humanitarian operations take place are cut off from the international banking system, MSPs continue to be a vital means of transferring funds across borders to field offices.

[19] Correspondent banks are third-party financial institutions that act as intermediaries for domestic and foreign banks engaged in cross-border payments but without a direct banking relationship.

Different types of MSPs

The money services sector consists of a diverse mix of providers with significant differences in terms of size, complexity and geographical coverage. They range from small organisations, such as grocery shops, convenience stores and pharmacies, to larger regional networks.[20] MSPs may specialise in other economic areas, including retail and wholesale, through which they accumulate cash pools that they use to pay customers. Digital payment solutions are not considered MSPs, although these also play an increasingly important role in the humanitarian response.[21]

MSPs may directly employ individuals who receive and pay out funds to customers, or they may enter into ad hoc contractual relationships with agents that operate as independent entities, the latter particularly in areas they do not regularly service. Multinational MSPs often operate extensive agent networks across many jurisdictions.

In-country use of MSPs

For in-country services used to pay CVA beneficiaries, organisations will contract MSPs that offer the best transfer method for the target population. In most settings, different transfer methods are available, including mobile money companies that use digital means of distribution, and formal and informal MSPs that distribute hard cash to staff and project participants. Organisations typically contract MSPs after issuing calls for tender for specific or recurring transactions and choosing the most competitive offer. They may also diversify distribution methods and sign framework agreements with different providers to be more resilient and flexible in crisis situations.

Cross-border use of MSPs

When using MSPs for cross-border transfers, organisations often send funds to neighbouring countries of their final destination or regional financial hubs where MSPs are registered. For cross-border payments to the north-western and north-eastern parts of Syria before the change of government in December 2024, MSPs typically received payments in Jordan or Iraq. According to some interviewees, many MSPs in the Middle East that work with humanitarian organisations have become more professional over the last decade, obtaining licenses from regulators in response to their partners' due diligence requirements.

To transfer funds to Afghanistan, MSPs are often paid in the UAE, Iraq or Pakistan after humanitarian organisations in the country have received the agreed amount. Organisations relied heavily on MSPs after the Taliban assumed power and the correspondent banking network connecting Afghan banks to the international financial system almost entirely collapsed.[22] Most interviewees said some banks had since resumed operations, enabling bank transfers to Kabul.

Many organisations continue to rely on MSPs for cross-border and in-country payments, however, given withdrawal limits imposed by the Afghan Central Bank and the limited reach of the domestic banking system, which leaves most rural areas unbanked. Some local NGOs rely on MSPs for cross-border transfers because they do not benefit from the humanitarian exemptions required by banks and are generally more affected by derisking.[23]

Some countries where humanitarian operations take place have taken steps to expand their banking infrastructure, but it is extremely unlikely that Afghanistan's and others in similar settings will mature enough to render MSPs redundant in the near future. This illustrates that MSPs are not just a short-term solution for acute crises, but in some settings a long-term tool for humanitarian organisations and unbanked and financially excluded people.

---

20 FATF, Guidance for a Risk-Based Approach for Money or Value Transfer Services, 2016.

21 More information on this topic can be found here.

22 More information on humanitarian organisations' financial access constraints in Afghanistan after the change in government in 2021 can be found here.

23 Banks may consider local NGOs higher risk clients than large INGOs, and the former have fewer resources to dedicate to risk management and compliance procedures. Some humanitarian exemptions only apply to a limited range of organisations. See, for example, the conditions limiting the scope of UNSC resolution 2664 and excluding many local NGOs.

Commission rates

The commission rates humanitarian organisations pay to MSPs differ substantially and may fluctuate rapidly depending on a number of factors. These include the availability of liquidity for MSPs, general demand for their services, their need to transfer money outside of the country, their size, the volume of the transaction, inflation and the risks they assume.

In most situations, rates range from three to four per cent and are often fixed in contracts for a certain period of time or number of transactions. In some cases, providers reportedly reduced their commission rate to zero to accelerate the movement of funds out of the country.

At the other end of the spectrum, rates may reach 15 per cent in acute crises when demand is high, accessibility is limited and MSPs pre-finance transfers for which they only get reimbursed upon receipt. Such increases took place in Myanmar, and in Syria after the earthquake in the country's north-west in February 2023. In extreme cases, most recently in Gaza and Darfur, rates may even exceed 25 per cent.

When assessing the commission rates paid to MSPs, it is important to take into account that they often offer lower exchange rates compared with central banks. Using MSPs that charge higher commission rates than banks, if available, may still be the cheaper option.

CASE STUDY:

NORTH-WEST SYRIA

Before the fall of Bashar al-Assad's government in December 2024, Hayat Tahrir al-Sham (HTS), a designated terrorist entity, controlled large areas of territory in the north-west of the country. According to the UN, 4.2 million of the 5.1 million people living in areas HTS controlled were in need of humanitarian assistance in 2024 before the start of its offensive. But there were no operational banks in these areas, making MSPs and cash carrying the only options for receiving and exchanging funds for humanitarian operations.

MSPs that received humanitarian funds were typically licensed and based in neighbouring countries, but their counterparts in north-west Syria were unregistered. Working with these providers was necessary, however, to reach people in need, and organisations used robust internal risk management measures, including making payments in arrears, to mitigate the risk of funds being diverted to designated terrorist groups.

Payment in arrears meant the MSPs had to accept the risk that humanitarian organisation may not be able to reimburse them the amounts paid out to project participants or field operations. Several interviewees reported significant delays in payments to MSPs, sometimes for as long as several years as a result of banks' refusal to process transactions involving such providers. In some situations, particularly for payments to beneficiaries of CVA programmes, MSPs paid cash-out agents up front and assumed all risks related to the agents' loss of funds.[24]

As of January 2025, the banking sector was still hesitant about processing transactions to Syria, despite the Office of Foreign Assets Control (OFAC)'s adoption of general license 24, which authorises transactions with government institutions, including payments to support the delivery of humanitarian aid.[25] As long as formal bank transfers to Syria and access to banks in all areas of the country are not possible, MSPs will continue to play an important role in sustaining the humanitarian response in the country.

[24] OCHA, Syria homepage, undated.

[25] OFAC, General License No.24, 8 December 2024.

KEY TAKEAWAYS

- **Default method to use banks and regulated MSPs:** Humanitarian organisations usually prioritise using the international banking system for transfers, but resort to MSPs when banking services are unavailable or inadequate, particularly in remote or conflict-affected areas. When using MSPs, they prefer registered over informal providers to minimise risks.
- **Cross-border and domestic payments:** Organisations use MSPs in two main ways: as alternatives to correspondent banking networks for cross-border payments; and domestic transfers, including to pay staff and run CVA programmes. Cross-border payments through MSPs are increasingly used because of derisking and the decrease of correspondent banking networks. They provide a vital lifeline to people in need who otherwise might not be reachable.
- **Diversity of MSPs:** The money services sector consists of a diverse range of providers with differences in terms of size, complexity and geographical coverage. MSPs employ different transfer methods, including mobile money companies using digital means of cash distribution.
- **Fluctuating commission rates:** MSPs' commission rates vary widely based on factors such as supply and demand, transaction volumes, the provider's size and the risks they assume. They can range between zero and 25 per cent. In most situations, they tend to be between three and four per cent, but they increase during emergencies.

2.3 SNAPSHOT OF DONOR POSITIONS AND POLICIES ON MSPS

All government donors interviewed for this research recognised the important role MSPs play in supporting humanitarian operations. They were seen as crucial to a timely response, to ensuring that organisations do not have to resort to riskier practices such as carrying cash and to enabling CVA programmes to reach beneficiaries in remote areas.

Various reports and statements by donor governments confirm this view. In response to a parliamentary question to the Foreign, Commonwealth and Development Office in September 2023, for example, the UK government stated:

"Money Service Businesses (MSBs), including Hawala, play an important role in conflict zones such as Afghanistan, Yemen, Sudan, Gaza and the Occupied Palestinian Territories. MSBs are often the only way of transmitting money, including remittances, to remote communities where formal banking services are limited ... Government guidance sets out clearly that hawala banking in the UK is legal and that many are regulated."[26]

The UK's Office of Financial Sanctions Implementation (OFSI) provides general guidance on how and when humanitarian organisations should use MSPs. It states that informal value transfer services "are sometimes used where there may be no formal banking facilities available, or where there are, there is limited access to them" and that "in the UK, Hawala banking is not illegal, and many are regulated by HMRC".[27]

The Charity Commission for England and Wales has also issued guidance on how charities should transfer funds abroad, including through non-bank financial service providers. It acknowledges "that charities may need to use these methods if banking facilities are not available" and says they should carry out "appropriate and proper due diligence to ensure the person or entity to which the charity is sending money is known and

[26] UK Parliament, Armed Conflict: Bank Services - Question for Foreign, Commonwealth and Development Office, 13 September 2023

[27] OFSI, Financial sanctions guidance for charities and non-governmental organisations, 21 June 2024, section 6.2.

trustworthy, and ensuring all the relevant regulatory issues have been considered and addressed by the trustees".[28]

These requirements are broad and allow for flexibility in accordance with the specific circumstances of transfers.

USAID confirmed in 2023 that its partners responding to the conflict and humanitarian crisis in Sudan were permitted to use "hawalas or unlicensed/unregistered mobile money providers to support payments" while relying on "licensed/registered banks and mobile money providers to the extent possible".[29] It also reaffirmed its partners' obligation to follow standard procedures, including the terms and conditions of their award, and reminded them to follow their own internal controls procedures, including "standardized checking of hawalas/mobile money providers against sanctions lists and other risk mitigation measures related to fraud, waste and abuse".[30]

ECHO also recognises the importance of MSPs in some humanitarian settings in a note to its partners:

"Some money transfer agents are registered with the central banks and hold licences authorising them to perform various financial transactions, others are long-established and operate under nationally accepted conventions and norms. In both cases, they are widely recognised and often operate in parallel and as a complement to the national banking sector … The money transfer system may, therefore, provide an essential service for displaced, unbanked and financially excluded populations and may contribute to mitigate the deepening of a crisis in a country."[31]

This statement demonstrates a clear understanding of humanitarian organisations' operational realities, particularly in rural and hard-to-reach areas with weak banking infrastructure, and the historical and cultural importance of MSPs in many parts of the world. It also indicates awareness that organisations use regulated MSPs whenever possible.

The use of MSPs usually falls under the general provisions for procurement processes within project guidelines and grant agreements. ECHO's note further specifies the conditions under which the costs involved are eligible.[32] Eligible commission rates are capped at five per cent of the overall transaction volume. This can support organisations in negotiations with MSPs and discourages them from charging unreasonably high rates but, as several interviewees pointed out, rates may reasonably exceed five per cent in some settings.

ECHO's guidance includes a requirement to use MSPs only if they are "a natural or legal person operating as a financial operator (including money services providers), in accordance with any applicable national law".[33] The broad formulation of "any applicable national law" could be interpreted as ensuring that providers are licensed by regulatory bodies, such as national central banks, but as discussed above registered MSPs will not be present in all humanitarian settings, particularly in areas controlled by non-state armed groups.[34]

---

28 Charity Commission, Compliance toolkit chapter 4: Holding, moving and receiving funds safely in the UK and internationally, November 2022.

29 USAID, Sudan guidance on use of hawalas, 28 June 2023.

30 *Ibid.*

31 ECHO, Note to echo partners implementing humanitarian aid actions in countries where the use of money transfer agents is needed, 7 November 2023.

32 *Ibid.*

33 *Ibid.*

34 ECHO should clarify in its guidance that in these exceptional circumstances aid organisations are permitted to use such providers. In locations where there are no laws regulating MSPs, ECHO's reference to compliance with 'any applicable laws' allows for their use.

Pre-approval and reporting

Some donors require humanitarian organisations to describe their intended use of MSPs during the proposal and planning stage of a project.[35] ECHO, for example, requires partners to submit an operational justification and an overview of risk mitigation measures, including those to reduce the risk of breaching EU restrictive measures and the diversion of funds to entities engaged in illicit activities.[36]

One donor was reported to have a policy under which the use of MSPs requires pre-approval, but has granted organisations exemptions if their internal policies demonstrate clear and effective risk mitigation measures. USAID's Bureau for Humanitarian Assistance (BHA) has adopted a policy that requires organisations planning to use an MSP in a high-risk area to submit its name for vetting.[37] Most interviewed organisations found BHA's approach useful because of its quick response time and because it provided them with additional reassurance about the reliability of specific providers. Some organisations shared BHA's written confirmations with banks, increasing their legal comfort and facilitating transfers to MSPs.

Another donor provided its partners with a list of pre-vetted MSPs with approved, partly approved and rejected providers. The list, however, was out of date and many of the greenlighted providers could not be reached and no longer seemed to operate. This affected organisations' ability to diversify their engagement with MSPs, reducing resilience and flexibility in case some providers faced liquidity constraints.

Some donors also require organisations to report regularly on their use of MSPs, including in interim and final reports. This may include providing invoices or other formal documentation as proof.

Ultimately, while exercising particular care over humanitarian organisations' use of MSPs, the donors interviewed for this guidance demonstrated a clear understanding of the essential role such providers play in safeguarding the provision of assistance in hard-to-reach and unbanked locations. ECHO's note and the UK government's guidance have been particularly useful in clarifying their partners' permission to use MSPs.

KEY TAKEAWAYS

- **Importance of MSPs:** Donors widely acknowledge the important role of MSPs in supporting humanitarian operations, particularly in conflict zones and remote areas where traditional banking services are limited or unavailable.
- **Guidance and requirements:** ECHO has issued the most comprehensive guidance on the use of MSPs. Rooted in an understanding of operational realities, it reaffirms their important role in the humanitarian response but also outlines requirements. These include that commission rates do not exceed five per cent of the total transfer volume and that providers are registered with competent national authorities, while allowing for exceptions if deemed necessary.
- **Vetting of providers:** Some donors have introduced vetting mechanisms for MSPs. USAID requires organisations to submit the names of MSPs and their owners used in certain high-risk locations for vetting. Another donor has produced a list of pre-vetted MSPs with partner organisations operating in certain high-risk locations. Humanitarian organisations report advantages and disadvantages with pre-approval systems.

---

35 BHA, for example, has made explicit reference to money transfer service providers in its risk assessment management plan, in the section outlining additional requirements for applications in high-risk environments. Full details can be found here.

36 ECHO, Note to echo partners implementing humanitarian aid actions in countries where the use of money transfer agents is needed, 7 November 2023.

37 More information on USAID's approach to partner vetting, including the vetting of MSPs used for the implementation of its awards, can be found here. USAID conducts partner vetting in Afghanistan, Iraq, Lebanon, Palestine, Pakistan, Syria and Yemen. Its power to require vetting of MSPs used for the implementation of its awards in certain locations derives from the US Foreign Assistance Act of 1961. More information can be found here and here.

2.4 RISKS AND CHALLENGES INVOLVED IN USING MSPS

Most donors and humanitarian organisations interviewed for this research emphasised the importance of adopting a holistic approach when assessing the use of MSPs. This entails weighing legal and reputational risks associated with using MSPs against those that arise from not having access to such providers, which may significantly delay or prevent the delivery of assistance.

One representative of a donor state said you "need to consider the risk of not meeting your foreign policy objectives if you have to halt aid because some places can only be reached through MSPs operating outside of the banking system". They said that normally any risks are "outweighed by the obvious benefits in humanitarian terms" and subscribed to a risk-based approach when assessing partners' use of MSPs.

Several representatives of donor states pointed out that using MSPs was much safer than some of the high-risk alternatives, such as carrying cash. One also emphasised that MSPs offered a viable lower-risk alternative to transfers through official banking routes in settings where state parties to a conflict are able to access and abuse data about the recipients of such transfers. In such settings, MSPs may be used not despite the risks, but in order to reduce them.

When humanitarian organisations use MSPs, they may be exposed to distinct operational challenges, including the risk that funds do not reach field operations or final beneficiaries on time, and legal and reputational risks associated with inadvertently violating sanctions or CT measures or facilitating money laundering.

2.4.1 OPERATIONAL CHALLENGES

One of the main operational challenges that may arise when using MSPs relates to working with banks to transfer funds to them. When asked to process transfers to environments and/or recipients considered high-risk, banks may hold them for extended periods while due diligence checks are completed. Challenges most often arise when using US dollars in transactions, given financial institutions' reliance on access to the US financial system and concerns about falling foul of extensive US sanctions and CT measures.[38]

Such delays have the potential to negatively affect the reputation of not only humanitarian organisations' reputation but also their work. Affected MSPs may halt or suspend their transfers, putting the implementation of programmes at risk. One organisation reported an incident in which banks had stopped transferring funds to an MSP, leaving it with a $1.5 million debt to the provider. The situation was ultimately resolved, but being unable to pay suppliers' invoices, including those of MSPs, can potentially put staff safety and security at risk. One organisation reported having faced pressure from providers, beneficiaries and local authorities, including physical threats to their staff in such a situation.

2.4.2 LEGAL AND REPUTATIONAL RISKS

The interviews conducted for this research highlighted three main legal and reputational risks humanitarian organisations may face when using MSPs.

1. **Aid diversion** was reported as a concern by some donors, but the risk of funds transferred through MSPs being diverted is minimal, given that most organisations pay in arrears once receipt has been confirmed. For CVA programmes, this includes beneficiaries verifying receipt of funds, sometimes reaffirmed by visiting them.

2. **Violation of sanctions or CT measures** poses a risk when working with MSPs in areas where designated entities and individuals are present. In some cases MSPs, or individuals known to own them, are themselves subject to sanctions.[39] Organisations mitigate these risks by subjecting the MSPs they contract to screening against sanctions lists, as they would with any other suppliers.

---

[38] In some settings the use of USD is unavoidable, because it may be the only currency MSPs accept or payments in another currency would incur significant foreign exchange losses.

[39] The EU, for example, has designated money service providers and/or their owners involved in financing Hamas and Islamic Jihad in Gaza. More information can be found here.

Flooded tents in Khan Younis, Gaza. © Amjad Al Fayoumi/NRC

3. **Money laundering** risks may arise, particularly if regulatory efforts and enforcement capacities are limited. Some MSPs generate the majority of their revenue in other sectors and have an interest in moving their funds to more stable jurisdictions, and working with humanitarian organisations is one potential means of doing so. Organisations interviewed for this paper include questions about the source of funds in their supplier vetting procedures for MSPs.

It is impossible to eliminate all risks when using MSPs to sustain humanitarian operations, particularly in locations with active conflicts or which are disconnected from the banking system. None of the risks involved, however, are unique to working with MSPs. They also exist in relationships with other service providers or suppliers.

That is why most donors rely primarily on procurement rules in project guidelines and grant agreements. Based on a shared understanding of the importance of working with MSPs, donors and humanitarian organisations have worked together to identify and implement risk mitigation measures in an effort to ensure that all assistance reaches its intended beneficiaries. The steps that humanitarian organisations have taken to do so are discussed in the next chapter.

KEY TAKEAWAYS

- **Holistic assessment of risks:** Donors and humanitarian organisations emphasised the importance of adopting a holistic approach to assessing the risks associated with the use of MSPs on the one hand, and those arising from not using their services on the other, including the delivery of assistance being delayed or prevented.
- **Operational risks:** Sending funds to MSPs in high-risk areas is often challenging because home banks or correspondent banks may be unwilling to process transfers, particularly when the currency is US dollars. Late payments to MSPs can disrupt humanitarian organisations' programmes, damage their reputation and even expose their staff to safety risks.
- **Legal and reputational risks:** Organisations face risks of aid diversion, sanctions violations and money laundering when using MSPs in unstable areas.
- **Residual risks:** It is not possible to eliminate all risks, particularly in challenging environments, but in line with their mandates humanitarian organisations work hard to manage them and ensure that all assistance reaches their intended beneficiaries.

3 GOOD PRACTICE

Humanitarian organisations have developed extensive expertise in collaborating with MSPs. They have established robust risk management practices and ways of working to ensure the highest levels of due diligence and efficiency, enabling the timely delivery of assistance to those in need. Based on the interviews conducted for this paper, this section discusses the good practices they have adopted.

3.1 TERMINOLOGY

NRC uses the term MSP rather than alternatives such as hawala, not only because it is more neutral, but also because it covers the wide range of providers that humanitarian organisations use, including multinational money service businesses, which are licensed and regulated in many jurisdictions, and more informal providers. As such, it serves as a useful umbrella term. Several other organisations said they refrained from using the term hawala for the same reasons.

3.2 BUILDING TRUST WITH DONORS AND BANKS

Humanitarian organisations generally follow procurement procedures that donors regularly review and approve when using MSPs. Donor interviewees said they were generally aware of when and how their partners used MSPs, but the level of that knowledge appeared to differ among them and within their agencies. Some said they appreciated organisations sharing information with them on the operational reasons for using MSPs and the risk mitigation measures adopted, particularly when doing so was new to a humanitarian response. Examples in recent years include Afghanistan, Myanmar and Sudan.

Information sharing builds trust and helps donor staff explain the importance of MSPs for humanitarian operations to their agencies. That said, some interviewees wanted more to be done to improve awareness of the issue within their agencies and other parts of government.

Some humanitarian organisations said they had sought clarification from donors that their risk management procedures were sufficient for commission rates to qualify as eligible costs, and that some donors had given written confirmation that they were permitted to use specific MSPs. They have, however, also rejected the use of providers that appeared to be linked to designated entities or individuals, or to be involved in money laundering or other suspicious activity, based on internal screenings.

Banks may consider organisations that work in areas affected by conflict high-risk customers. Many interviewees underscored the importance of maintaining a trust-based relationship with banks and a commitment to transparency. This includes regular information sharing on organisations' internal risk mitigation measures and avoiding "wire stripping", the practice of minimising or altering the provision of information on the origin and/or destination of funds.

Organisations reported using different approaches to information sharing with banks when using MSPs, some doing so proactively and others upon request from the bank. Organisations with particularly strong compliance departments said their banks regularly processed transactions to MSPs for them. They almost exclusively relied on registered entities or intermediaries that only work with MSPs after subjecting them to stringent due diligence procedures, or they were able to share letters with banks from donors confirming they were permitted to use specific MSPs.

Humanitarian organisations and banks may have different understandings and methods for information sharing, but the organisations interviewed all said they were aware of the importance of maintaining transparency with the banks processing their transfers, including about the destination of funds.

KEY TAKEAWAYS

- **Building trust with donors:** Donors appreciate humanitarian organisations sharing information proactively about using MSPs, particularly in settings where it had previously not been necessary to do so. In turn, some donors have supported organisations with written confirmation of approval for their use.
- **Building trust with banks:** Banks have repeatedly expressed concerns about the use of MSPs and have rejected transfers to some providers. This risk can be mitigated in part by sharing approval letters from donors and other information on humanitarian organisations' internal risk mitigation measures.

3.3 RISK MITIGATION MEASURES

Humanitarian organisations that use MSPs to support their operations generally adopt a range of risk mitigation measures, many of which exceed legal requirements or commitments in grant agreements with donors. Given, however, that a zero-risk approach is not feasible, it is good practice to share residual risks across the stakeholders involved rather than passing them on to local partners or beneficiaries.

Some organisations employ dedicated compliance staff, which facilitates a closer working relationship with their counterparts in banks, including by regularly sharing information on internal risk mitigation measures for using MSPs and other suppliers. However, only large organisations are able to afford such measures.

All organisations interviewed for this research said they had adopted mitigation measures in line with the risks associated with certain MSPs. Risk assessments are made on a case-by-case basis before signing contracts with providers. Key risk mitigation measures include using registered MSPs where possible, following standard procurement policies, adopting specific know your supplier (KYS) procedures, subjecting MSPs to CT/sanctions screening and making payments in arrears. These are outlined in more detail below.

Other measures include signing contracts with providers, making large payments in tranches and running test payments with small amounts when using new providers.

3.3.1 ROBUST PROCUREMENT POLICIES AND PROCEDURES

Contracting MSPs falls under humanitarian organisations' general procurement policies, which are generally aligned with donors' requirements and approved by them. The policies assign roles and responsibilities on the safe use of MSPs. Implementation may involve a range of staff, from logistics and finance to risk, legal and compliance teams, and senior management when payments exceed certain thresholds.

Interviewees emphasised the essential role of colleagues in the country of operations in assessing MSPs' suitability, including through direct interviews, discussions with local community members or information sharing in coordination bodies, such as national cash working groups, to ensure compliance with procurement rules.

Procurement policies may require organisations to publish a tender for MSPs' work. In some settings, however, only a limited number of providers may be available and they may not be able to meet the procurement requirements, including the provision of documentation. In such cases, a derogation from the standard requirement to receive at least three bids may be accepted.

Annex 1 is an excerpt from the procurement policy of one of the humanitarian organisations that participated in this research. It provides guidance on working with formal and unregistered suppliers, including MSPs. General internal procurement procedures may be supplemented with specific guidelines or KYS procedures to streamline awareness of associated risks and mitigation measures.[40]

[40] The Center for Operational Analysis and Research has published a checklist of policies and procedures humanitarian organisations working with MSPs in Myanmar should have in place. More information can be found here.

KEY TAKEAWAYS

- **Humanitarian organisations' procurement policies:** Internal procurement policies aligned with donor requirements ensure the safe use of MSPs, outlining the roles and responsibilities of staff and selection criteria, including cost and the provider's financial stability, performance and ability to meet the requested timeline.
- **Exceptions to procurement policies:** Derogations from standard requirements are only acceptable in extreme situations in the absence of MSPs that are able to comply.

3.3.2 USING REGISTERED MSPS WHERE POSSIBLE

Interviewees said there had been a move towards formalisation among MSPs over the last decade in response to a growing awareness of humanitarian organisations' compliance policies and donor requirements. Sometimes MSPs may actually be better regulated than the banking sector. One donor said this is the case in Somalia, where the banking sector is relatively small in terms of market size and transfer volumes, and MSPs "have been regulated for longer and have better levels of compliance". Nearly all cross-border payments go through MSPs registered with the country's central bank as a result.

One donor and one humanitarian organisation said that in some situations using registered MSPs could pose security risks because it could allow authorities to track transfers and access beneficiary data, meaning that it was better to use unregistered providers. For the most part, however, the MSPs that organisations use are regulated in the jurisdictions they operate in.

This is typically required by organisations' donor-approved internal procurement policies, unless no such providers are available. The internal procurement policy of one organisation interviewed states that "every effort needs to be made to make sure that all suppliers that [the organisation] works with are formal/registered suppliers" (see Annex 1 for full excerpt). The policy goes on to say that formal suppliers, including registered MSPs, can be identified by their ability to provide the following information and documentation:

- Legitimate business registration for trading and tax, as per local legislation
- Proof of registered physical addresses
- Formal identification documents for owners
- Company bank account details

It stipulates that the organisation has to accept bids from registered providers even if they carry acceptably higher costs than those from unregistered providers, but it also acknowledges that "in some context [sic] and due to the nature of [the organisation]'s work, it may happen that no formal/registered suppliers are available for certain types of products". The organisation is only allowed to use an unregistered supplier "if the technical and/or financial offer is considered instrumental or fundamental in achieving the project objectives or will make significant difference in terms of best value for money".

Interviewees for this research indicated that the starting point for humanitarian organisations working with MSPs is to examine the kind of licence they can produce. Some indicated regularly involving legal or risk and compliance staff or external legal counsel more familiar with applicable national legislation. This can help determining whether the licence is valid for the provision of financial services. Central banks or finance ministries tend to issue such licences. Given the multinational reach of MSPs that offer cross-border transfers, it is advisable to ask them to provide licences for all relevant jurisdictions.

A CARE International paper on using *hawala* for cash programming in Syria, however, states that the organisation no longer requires MSPs to prove registration as a financial service provider, but accepts company registration and a general trading license. It also notes that "only the large *hawala* companies ... have the capacity to provide the needed information for due diligence checks".[41] This may include large businesses with excess cash that are not formally registered as MSPs. In settings where no registered MSPs are present, organisations need to be prepared to exercise the flexibility shown by CARE.

[41] ALNAP, Using Hawala to conduct cash programming in Syria, 1 January 2019.

KEY TAKEAWAYS

- **Preference for registered MSPs:** Humanitarian organisations use registered MSPs whenever possible to ensure legal compliance and mitigate risks. Exceptions may apply if such providers are unavailable, particularly in high-risk areas, allowing organisations the flexibility needed to sustain their operations.
- **Formalisation of MSPs:** Many MSPs are increasingly formalised and compliant. According to one donor, MSPs in Somalia are more reliable than the banking sector, making them the safest choice for cross-border payments.

3.3.3 KYS PROCEDURES

As part of standard procurement procedures and any specific KYS procedures for working with MSPs, humanitarian organisations have measures in place to verify their identity and gather information to assess the risks associated with entering into a business relationship (see previous section). They may also contact references provided by the supplier, request their own references from other NGOs or UN agencies, verify any licences provided with the issuing authority and make an unannounced visit to the provider's office to ensure the address exists and is legitimate.

Interviewees said a clear overview of all agents/providers in a payment chain could be an effective measure to mitigate the risk of facilitating money laundering or financing terrorism. Establishing such an overview, however, is very time-consuming and often not feasible if an MSP's ownership and control structures are unclear. Simultaneously, the challenges associated with understanding suppliers' ownership and control structures are not limited to MSPs but can involve any business humanitarian organisations work with. In this regard, one interviewee from a donor agency said donors could do more to use their internal knowledge and intelligence capabilities and share information about suspicious providers with their partners.

Some organisations have internal approval procedures, in which country office staff gather some of the information outlined above and then ask the treasury/finance team or senior management in head office to approve an MSP's use when a particular level of risk or transfer volume is involved. This centralised approach adds an extra layer of protection, but it is only feasible if the teams in question are appropriately resourced. This underscores the importance of ensuring that organisations are well resourced, including the training of staff, if necessary, to implement their compliance policies.

KEY TAKEAWAYS

- **Verification and risk assessment:** Humanitarian organisations follow standard KYS procedures to verify MSPs' identities, which include checking registration documents, owner identification and bank details, and conducting site visits. They also gather references, especially from NGOs and UN agencies, and verify licenses.
- **Internal approval processes:** Some organisations employ centralised approval processes for added risk mitigation, highlighting the need for adequate resources to uphold these compliance measures.

3.3.4 CT/SANCTIONS SCREENING

Another component of humanitarian organisations' standard procurement policies is to screen service providers, including MSPs, against sanctions and CT lists before signing contracts. Taking steps to ensure that sanctions or CT measures are not violated is standard practice in the aid sector and a basic requirement for the majority of donors and certification bodies. To screen providers, organisations must obtain the full names and identification documents of their beneficial owner(s) and any agents.

Larger organisations may be able to afford sanctions screening software, such as Bridger or CSI WatchDOG, which run checks against

consolidated global sanctions and CT lists.[42] Others run manual checks or use a free/low-cost service such as OpenSanctions.[43]

All of the humanitarian organisations interviewed said they rarely if ever had any matches when screening MSPs' owners and agents. As section 2.4 shows, however, the EU and US have targeted certain MSPs and their owners in recent years. This demonstrates that while sanctions screening is an important risk mitigation measure, organisations' procurement processes are likely to filter out MSPs associated with listed entities or individuals before the screening stage.

KEY TAKEAWAYS

- **Sanctions and CT screening:** Humanitarian organisations incorporate sanctions and CT screening into their procurement policies for MSPs. Larger organisations use specialised software, while smaller ones may rely on free/low-cost options or manual checks.
- **Effectiveness of procurement practices:** Some MSPs have been sanctioned by the EU and US, but interviewed organisations said they rarely if ever had any matches when screening. This indicates that standard procurement practices filter out high-risk providers before the screening phase.

3.3.5 PAYMENT IN ARREARS

Humanitarian organisations often have contractual arrangements with MSPs to pay them in arrears to mitigate aid diversion risks.[44] Doing so is particularly important if the relationship with an MSP is new or when the provider is not licenced to operate as a financial service provider and options for legal recourse are limited. When signing contracts with MSPs that accept payment in arrears, organisations must be aware of their responsibility to reimburse on time to avoid penalties and related risks.

Many MSPs have been providing their services for many years and have developed trusting relationships with NGOs and UN agencies. In this case, or in situations in which no provider offers to be paid in arrears, organisations may make advance payments. Associated risks are assessed on a case-by-case basis.

It appears that organisations' current approaches are generally effective in mitigating the risk of funds being diverted, because no interviewed organisation said they had lost funds when working with MSPs. Donor interviewees said they generally expected their implementing partners to make payments to MSPs in arrears, while acknowledging that in exceptional cases advance payments were permitted.

KEY TAKEAWAYS:

- **Payment of MSPs after receipt of funds:** Humanitarian organisations often pay MSPs in arrears, which minimises risks, especially with new or unlicensed providers. Advance payments are generally only made when other options are unavailable and the organisation has a trusted relationship with the provider.

3.3.6 DIVERSIFYING ENGAGEMENT WITH MSPS

Most humanitarian organisations interviewed for this research emphasised the importance of diversifying engagement with MSPs to maintain leverage and flexibility during crises. This was also illustrated in CARE's paper on the use of

---

42 LexisNexis, Bridger Insight homepage, undated; CSI, WatchDOG Elite homepage, undated.

43 OpenSanctions homepage, undated.

44 Aid diversion refers to instances when assistance does not reach the intended recipients because of interference, fraud, theft or damage by a government, local authority, armed group or other actor. It is involuntary, unintended and not permitted under humanitarian exemptions. As such, it is notably different from "incidental benefits", which describe funds and/or resources provided to designated individuals or entities, including via the payment of taxes or the use of a particular supplier. Exemptions such as UNSC resolution 2664 and some in states' autonomous sanctions regimes permit incidental benefits if required for the provision of humanitarian assistance. Some donors have explicitly allowed for the use of MSPs subject to sanctions if absolutely necessary and covered by a corresponding exemption.

MSPs in the cash response in Syria.[45] A large proportion of the humanitarian funds entering areas not controlled by the government were transferred via the same few hawala providers, creating substantial operational risks if any of them ceased their operations.

To mitigate this risk, many organisations said they checked regularly for other competitive providers and signed framework agreements with a range of reliable MSPs, stipulating commission rates for a limited amount of time and/or number of transactions. This does not oblige organisations to use a provider, but it provides flexibility. If one MSP is facing liquidity shortages or other challenges, they can quickly pivot to other providers and ensure their staff and suppliers continue to receive payments on time and that their programmes are not interrupted.

One organisation, for example, said it tended to rely on mobile money providers in Iraq, but also had agreements in place with MSPs. At the height of the Covid-19 pandemic, this allowed it to shift from mobile providers, which were heavily affected, to MSPs, thereby ensuring its operations received vital funds. Another organisation said it had signed contracts with more than 10 MSPs in Sudan, ranging from large businesses to providers offering digital payment solutions.

KEY TAKEAWAYS

- **Diversifying MSP engagement for crisis resilience:** To maintain flexibility and reduce operational risks, humanitarian organisations are advised to engage with a number of MSPs using framework agreements, which set terms without guaranteeing work. This allows swift shifts to alternative providers if one faces issues, ensuring timely payments and uninterrupted operations during crises, as illustrated by organisations working in Iraq, Sudan and Syria.

3.3.7 CVA RISK MITIGATION MEASURES

When using MSPs domestically for cash delivery as part of CVA programming, humanitarian organisations adopt specific risk mitigation measures. According to interviewees, some involve the local community in the selection of providers, including by conducting interviews with trusted members about their reliability. Selection is made, at least in part, based on the acceptability of an MSP to the people humanitarian organisations are accountable to, making it a participatory approach that also helps to ensure a provider's reliability.

Aid diversion risks in CVA programmes that rely on MSPs tend to be mitigated by collecting confirmation of receipt from beneficiaries. This may be done directly on site, through the MSP chain or by digital means. Only once confirmations are received is the MSP reimbursed. Aid diversion risks can be further reduced by post-distribution monitoring mechanisms, feedback mechanisms and being present regularly in the places where assistance is provided.[46] Country-specific risks can be addressed in cash working groups.[47]

KEY TAKEAWAYS

- **Risk mitigation in CVA programmes:** When using MSPs for CVA, humanitarian organisations often consult local communities to select trusted providers. They also manage aid diversion risks by obtaining confirmation of receipt from beneficiaries before reimbursing MSPs, post-distribution monitoring, feedback mechanisms and presence in the places where assistance is provided.

---

45 ALNAP, Using Hawala to conduct cash programming in Syria, 1 January 2019.

46 Further information from CALP on implementing effective post-distribution monitoring mechanisms can be found here, particularly p.22-23 and p.27-28.

47 CALP, Cash working group search page, undated.

A girl displaced from Khartoum, Sudan, playing in the afternoon sun. © Ingebjørg Kårstad/NRC

3.4 KNOWLEDGE SHARING ON MSPS

Interviewees from several humanitarian organisations said they regularly attended meetings of formal coordination forums, such as cash working groups and cash consortiums, or informal groups at both the country and global level to share knowledge about their use of MSPs. This includes the providers available, their capacity and reliability, their advantages and limitations, challenges with making bank transfers to MSPs and legal requirements in destination and transit countries. It may not always be easy to establish an overview of applicable law in some settings, and other organisations may offer helpful information.

Several interviewees also said they regularly exchanged information on commission rates in cash working groups. Doing so can facilitate negotiations to reduce rates, particularly when many organisations rely on the same MSPs.[48] One donor said they encouraged their partners to compare commission rates during crises to pre-crisis rates to make sure MSPs had not taken advantage of the situation and jointly inflated rates.

Cash working groups can be a useful source of institutionalised knowledge, but some organisations have preferred to coalesce more loosely in informal groups during specific crises, such as the change of government in Afghanistan in 2021 or the civil war in Syria, when they relied heavily on MSPs to run cash programmes and sustain their operations more generally.

KEY TAKEAWAYS

- **Knowledge sharing:** Humanitarian organisations regularly participate in formal and informal forums to share information on the national regulatory landscape, donor positions, commission rates, operational challenges and experiences of working with specific MSPs. Doing so helps to leverage joint knowledge in rapidly changing situations.

[48] This is also one of CARE's recommendations in its paper on humanitarian organisations' use of hawala for cash programming in Syria.

4 RECOMMENDATIONS

4.1 FOR HUMANITARIAN ORGANISATIONS

#1 When referring to MSPs, use neutral terms that reflect the diverse range of non-bank financial service providers humanitarian organisations use, including registered and unregistered entities.

#2 Ensure staff have clarity on donors' positions and policies on the use of MSPs. Consider institutionalising existing knowledge of the issue and making it available to relevant staff.

#3 Share information about the use of MSPs proactively with donors and banks. For banks, information sharing on humanitarian organisations' internal risk mitigation measures and donor letters permitting the use of MSPs may be important to build trust and facilitate transfers to MSPs.

#4 Use registered MSPs whenever possible. Providers should ideally be able to show proof of formal registration with competent authorities, such as the central bank or another supervisory body in all jurisdictions in which it interacts with your organisation. At the same time, allow exemptions in locations where registered providers are unavailable and consider requesting other forms of documentation that demonstrate government oversight, such as tax registration.

#5 Verify the identity of MSPs you plan to work with and gather information to assess any risks associated with entering into a contractual relationship with them. This is a standard requirement in procurement policies and may be supplemented by KYS procedures. Steps include checking registration documents, owner identification, source of funds and bank details, conducting site visits and gathering references from other NGOs and UN agencies. If intermediaries are involved in an MSP's payment chain, obtain information on them too, where this is possible. A list of possible questions to ask as part of KYS procedures is included in annex 2.

#6 Screen MSPs you work with against sanctions and CT lists before signing contracts. This is also part of standard procurement policies. To screen, organisations must have the full names and identification documents of a provider's beneficial owner(s) and any agents.

#7 Pay MSPs in arrears whenever possible, and particularly when working with new or unlicensed providers. Advance payments are generally only made when other options are unavailable and the organisation has a trusted relationship with the provider.

#8 Diversify engagement with MSPs. Check for competitive providers regularly, and sign framework agreements with a range of reliable MSPs to reduce reliance on individual providers and preserve flexibility during crises.

#9 For CVA programmes, consult local communities and select MSPs that beneficiaries trust. As part of sector standards, also reduce aid diversion risks by obtaining confirmations of receipt from beneficiaries before reimbursing MSPs and conduct post-distribution monitoring.

#10 Share knowledge on the use MSPs via cash working groups and other formal and informal forums. This may include information on the national regulatory landscape, donor positions, commission rates, operational challenges and experiences of working with specific MSPs.

4.2 FOR DONORS

#1 Continue to address bank derisking to ensure humanitarian organisations have access to financial services provided by registered banks. Adopt humanitarian exemptions in sanctions and CT measures and continue dialogue with financial institutions and national regulators with the aim of reducing organisations' reliance on MSPs.

NRC teams distributing multi-purpose cash assistance to people who have been displaced to the Al Houri camp in Gedaref, eastern Sudan. © Ahmed Elsir/NRC

#2 Allow humanitarian organisations to use MSPs for cross-border payments to transfer operational funding and for domestic payments. This should include the use of unregistered providers when necessary. Ensure that procedures facilitate organisations' timely use of MSPs, given the urgent nature of humanitarian programming.

#3 Work with other donors to establish a stronger collective position on the safe use of MSPs, with the aim of aligning policies on the issue. The Donor Cash Forum (DCF), hosted by the CALP Network, could play a useful role in fostering such a common position.

#4 Limit the pre-approval/vetting of MSPs to high-risk locations and ensure that procedures have quick turnaround times. Where possible leave it to humanitarian organisations familiar with the local situation to submit potential providers for assessment.

#5 Consider issuing approval letters stating that an organisation is permitted to use a specific MSP if it experiences derisking challenges when making payments to the provider's accounts. Such letters can also be used to increase banks' legal comfort more generally.

#6 Refrain from imposing unrealistic limits on eligible commission rates. Humanitarian organisations share donors' commitment to ensuring the most efficient use of funds. If limits are introduced, allow for exceptions, given that MSPs may sometimes charge high fees to be able to continue operating in hard-to-reach areas. Processing exception requests should take into account the urgent nature of humanitarian programming.

#7 Do not overburden organisations with information-sharing requests about their use of MSPs in addition to other reporting requirements. When asking for reporting on MSPs, ensure clear definitions are used, clarifying which providers fall under these requirements.

#8 Consider allocating additional resources to organisations' compliance teams to equip them with the required capacity and expertise to engage more closely with their counterparts in banks to improve banking options and reduce reliance on MSPs.

#9 Consider allocating support for coordination mechanisms that pool organisations' joint knowledge of using MSPs in rapidly changing settings and work towards maximising cost-effectiveness and managing risks effectively.

#10 Raise awareness of the reasons for which humanitarian organisations use MSPs, the legal frameworks governing their use and examples of good practice by organisations, donors, government departments and parliaments. This is important to address persistent misconceptions about organisations' ability to use MSPs safely and responsibly while promoting a better understanding of the limited risks involved. Also highlight the positive impact MSPs have had on organisations' ability to provide humanitarian assistance.

ANNEX 1:

EXTRACT OF AN ORGANISATIONAL PROCUREMENT POLICY ON WORKING WITH BOTH REGISTERED AND UNREGISTERED SUPPLIERS

This is an excerpt from the internal procurement policy of one of the humanitarian organisations that participated in this research. It sets out guidelines for working with formal and unregistered suppliers more generally, including MSPs, and criteria for choosing MSPs in cash programming.

FORMAL AND UNREGISTERED SUPPLIERS

The high prevalence of informal/unregistered suppliers in areas that [the organisation] typically operates in presents significant risks. Working with informal suppliers limits our ability to:

- identify fake suppliers,
- conduct due diligence checks,
- seek recourse via the legal system.

Every effort needs to be made to make sure that all suppliers that [the organisation] works with are formal/registered suppliers. In some context and due to the nature of [the organisation's] work, it may happen that no formal/registered suppliers are available for certain types of products in some specific areas or point in time.

While regulations vary from country to country, formal suppliers can normally be distinguished by being able to produce the following:

- Legitimate business registration for trading and tax, as per local legislation,
- Proof of registered physical addresses,
- Formal identification documents for owners,
- Company bank account details.

In addition to requesting the aforementioned supporting documentation, it is recommended to carry out the following additional controls:

- Independently contact references provided by the supplier and request written feedback with an emphasis on NGOs and UN agencies.
- Independently verify the details provided by the vendor with the issuing authority (Chamber of Commerce or similar authority). Physically visit the site of the supplier to ensure that the address that has been provided actually exists and is legitimate. In areas with high risk of corruption, it is good to make un-announced visits.

It is recognised that the aforementioned can be very time-consuming (especially the physical visits); they can however be instrumental in uncovering serious frauds/abuses. It is recommended that each country office approaches the problem in a reasonable way given the level of risk in the specific context/ market segment. If it is not possible to systematically carry out controls on all vendors, then efforts are concentrated on the areas that represent the highest risk of corruption (large contracts/markets which are characterised by the presence of a lot of informal actors, etc.).

DEALING WITH UNREGISTERED SUPPLIERS

It has been noticed that across [the organisation's] operations it is not always possible to find formally registered suppliers due to the political and socio-economic contexts. In particular, procurement of certain type of goods/services from registered suppliers proves to be a challenge. Where it is not possible to find formal suppliers, the unregistered supplier is required to submit formal identification documents and ideally proof of a permanent address. In these cases, it is strongly recommended that site visits are carried out before the evaluation process is finalised.

At the procurement evaluation stage, the committee should always give reasonable preference to registered companies, which should be selected even with an acceptable higher financial offer. The committee should select bids from unregistered suppliers only if the technical and/or financial offer is considered instrumental or fundamental in achieving the project objectives or will make a significant difference in terms of best value for money. The selection of unregistered bidders should be documented in the bid analysis form/tender minutes or similar document in line with relevant procurement thresholds or in an ad hoc note to file. The committee is always entitled to seek further legal advice from [the organisation's] country office legal adviser as deemed appropriate.

CRITERIA FOR CHOOSING A TRANSFER SERVICE PROVIDER

Many criteria are considered according to the local context and situation in which the cash-based intervention is implemented. Primary criteria are defined as follows, though this list is non-exhaustive and is contextualised:

- The service supplied safeguards the safety and security of [the organisation's] staff.
- The service supplied establishes coverage and ease of attainability for beneficiaries/shops.
- The service supplied guarantees comparative cost efficiencies, based on transfer costs/charges.

There are additional criteria to choose a transfer service provider. Again, the following list is non-exhaustive and contextualised:

- The service provider represents a socially responsible business.
- The service provider is registered and part of an approved financial arrangement.
- The service provider is capable of providing guarantee against loss of resources.
- The service provider is known and trusted by the recipients and other stakeholders.
- The service provider is non-discriminatory against women and marginalised groups.
- The service provider offers competitive service fees (transactions, account, cards, etc.).
- The service provider is able and willing to customise and develop necessary services.
- The service provider has experience in delivering payments to humanitarian and development programme recipients, social assistance, pensions, salaries, etc.
- The service provider operates and has the expertise for delivering payments in urban and rural areas.
- The service provider is capable of organising on-site delivery.

ANNEX 2:

OVERVIEW OF INFORMATION AND QUESTIONS TO ASK FROM MSPS AS PART OF THE KNOW YOUR SUPPLIER (KYS) PROCESS

This table provides an overview of some of the information humanitarian organisations may seek to obtain from MSPs as part of their KYS procedures. The questions can be adapted depending on the resources available to an organisation to obtain and process information, an MSP's anticipated risk level and its ability to provide information. According to the interviewees, only large MSPs tend to be able to respond to such detailed requests for information.

Theme	Questions
Registration: Formal registration with competent national authorities is a key factor in assessing the risks associated with an MSP. In most jurisdictions, registration comes with a range of obligations, including their own Know your customer (KYC) procedures and compliance with AML and CFT legislation and sanctions regimes.	• What is the legal status of your company? Please specify date and place of registration. • If your company is unable to register with competent authorities, why not? • Is your organisation permitted to provide financial services? If so, please provide confirmation of the business registration for trading and tax. • Please provide the identification documents of the owner(s) of your business. • Please provide proof of the registered address of your business.
References: Positive references from other NGOs and/or UN agencies are an important indication of an MSP's reliability.	• Can you provide any references from other NGOs and/or UN agencies you have worked with?
Maturity of the business and its owners' experience: This examines whether the provider is a new or established operation, its management's experience, and whether money services are its primary business.	• Since when has your business been providing financial services? • Are financial services your primary business?
Location(s) and market(s) served: Terrorist financing and money laundering risks may differ depending on location, customer base and markets served. Clarify whether markets served are domestic or international, and whether services target local residents or broad markets. It is also important to understand if an MSP has associations with other jurisdictions through headquarters, operating facilities, branches or subsidiaries. A visit to the place of business may be helpful to confirm its existence and activities.	• In which jurisdictions do you provide financial services? Does your business have a physical presence in these locations? • Do you hold licences to operate as a financial service provider for each jurisdiction? If not, why not?
Ownership and control: It is essential to acquire beneficial ownership information, in other words information about the people who own or control the business, whether directly or indirectly. This is important for effective screening against sanctions and CT lists.	• Who owns your business? • Can you provide a list of your business's board members?
Unlawful behaviour: Gaining an understanding of past illegal activities and legal actions against an MSP helps to assess any risks associated with working with it.	• Has your business been investigated, charged, convicted or otherwise involved in criminal, corrupt, unethical or illegal activities in the past 15 years? • Is there any pending legal action against your business?

Political affiliation: It is also important to understand any political affiliations an MSP may have that could compromise the perception of a humanitarian organisation's neutrality and independence.	• Does any government entity or other political actor have any financial, management or controlling interest in your organisation? If so, please provide details and level of interest.
Risk management: Asking an MSP to share information about its internal risk management processes helps to get a better understanding about its level of formality and the risks associated with working with it.	• Do you have an anti-fraud and anti-bribery policy? If not, what steps do you take to mitigate these risks? • Do you have a counterterrorism policy? If not, what steps do you take to mitigate these risks? • Do you have an anti-money laundering policy? If not, what steps do you take to mitigate these risks? • Do you have a data security policy? If not, what steps do you take to mitigate these risks? • How do you mitigate security risks when delivering cash to recipients?
Payment method and payment chain: MSPs sometimes rely on a network of agents to make funds available in the destination location. This may involve individual external agents, other MSPs or company employees. Try to obtain information about the entire payment chain to subject all of those involved to screening against sanctions and CT lists. MSPs that accept payment by bank transfer are likely to be formalised than those that only accept cash, because they will have had to go through their bank's KYC process.	• Who is the person/entity that delivers funds at the pay-out location? Are they a staff member/part of your business? If not, is this a new or established business relationship? • How do you settle payments with your agents – cash courier, trade, bank transfer, third party settlement? • Are there any intermediaries involved in the payment chain? If yes, please provide a list of all the agents/MSPs involved and their registration status. • Do you accept bank transfers or only cash? In which countries do you receive bank transfers?
Finance and liquidity: This is to obtain more information about an MSPs' capacity to cope with a humanitarian organisation's transfer requests, and ensure it is solvent.	• What is your average transaction size? What is the limit? • Are your accounts certified annually? Please provide the statutory audit reports of the past two years. • Are you registered for tax? Please provide proof.

NRC

NORWEGIAN
REFUGEE COUNCIL