Reporting guidance for EMIs

This additional example is part of the CGAP Technical Guide, *Digital Financial Services for Financial Inclusion: Tools for Supervisors.* It provides a practical illustration produced during CGAP's work with several country supervisors on DFS supervisory frameworks. This document is part of the Technical Guide's collection of Additional Examples and Guidance. Its utility and applicability to specific country contexts depends on factors such as the availability of data and other resources, the stage of development of DFS markets, experience with risk-based supervision, and institutional arrangements for supervision.

Contents

Purpose of this additional example

This additional example is a redacted and anonymized version of the reporting guidance prepared by a country's DFS supervisor for the EMIs that are subject to reporting requirements within its jurisdiction. It illustrates the types of EMI data that supervisors collect and analyze and the guidance supervisors may provide to EMIs.

It is important to note that the DFS supervisor that prepared the original document uses traditional data collection methods, such as Excel data templates, but has put in place internal rules for data validation and consistency. The country's reporting requirements focus on standardized aggregated data, which is typically reported on a monthly basis. Also note that terms used are the ones specifically used in that country.

For the above reasons, it is important that supervisors using this additional example adapt it to their particular context, adjusting the terminology and data formats and formulas, in consultation with EMIs. Also, if the supervisor has acquired supervisory technology (suptech) capacity or is planning to invest in suptech to revamp its data collection mechanism, the granularity and frequency of data collection can substantially increase and data validation can be automated to a great degree. Suptech solutions can also facilitate reporting by integrating the supervisor's data collection system with the EMI's operational system rather than basing reporting on EMIs inputting data into Excel templates.

1. Institutions required to report

Nonbank e-money issuers. However, this framework could also partially apply to banks—but only in regard to the e-money accounts they issue.

2. Overview of the reporting framework

- Report 1 (R1): E-money Account Numbers and Balances and Trust Accounts
  - Table 1.1. Total e-money accounts
  - Table 1.2. E-money accounts: End user
  - Table 1.3. E-money accounts: Agents
  - Table 1.4. E-money accounts: Other corporate
  - Table 1.5. Fund safeguarding/trust accounts
  - Table 1.6. Change in number of e-money accounts
- Report 2 (R2): Agents, Distributors, and Merchants
  - Table 2.1. Agents
  - Table 2.2. Other corporate: Merchants and distributors
  - Table 2.3. New agent appointments

- Report 3 (R3): Transaction Volumes and Values
  - Table 3.1. Cash-in and cash-out
  - Table 3.2. Transfers
  - Table 3.3. Purchases and payments
  - Table 3.4. Inward remittances
  - Table 3.5. Total transactions
- Report 4 (R4): Risk Incidents
  - Table 4.1. Pending transactions and loss from fraud and data security breaches
  - Table 4.2. Fraud and data security breaches
  - Table 4.3. Disruptions

3. Additional reporting

The standardized data contained in reports R1, R2, R3, and R4, outlined above, may be complemented by other types of data sources and both periodically reported to the supervisory authority or collected on an ad hoc basis. For example:

Detailed trust account statements. In addition to the data on trust accounts R1 requires, EMIs and banks may be required to submit full bank statements of each trust account holding e-money float (e.g., on a monthly basis). Statements must show balances, all transactions conducted in the month, interest earned in trust accounts in the month, and interest accumulated in the account.

Retail payment statistics. Reports R1–R4 are not a substitute for periodic reporting of statistics on payment instruments and channels (e.g., mobile banking, internet banking, ATM, POS, remittances). These are usually collected by the central bank or other payments regulator.

Unstructured data required by regulation. Reports R1–R4 are not a substitute for any other information obligation defined in applicable regulations. For instance, EMIs may be required to send information on IT infrastructure changes, changes in shareholder composition, and other changes as soon as it is available.

Ad hoc information requests. Likewise, R1–R4 do not substitute data and other information supervisors may require in the course of their supervisory activities.

4. Frequency of reporting

In countries with a substantial e-money industry, R1–R4 are typically required on a monthly basis.

5. Reference date

Reports should be filled out with data that reflects the EMI's situation at the business's close on the last day of each month. For example, if a company's business closes at midnight on May 31, the data reported will reflect May 31, midnight.

6. Time-to-report

Reports should be submitted by the fifth business day after the end of each reporting month. For example, for the May 2023 report, the submission deadline is Wednesday, June 7—based on data from Wednesday, May 31.

7. Method of reporting

Reports must be submitted through [*omitted in this anonymized version*], following the specific instructions and access information provided in [*omitted in this anonymized version*].

8. Validation

EMIs are required to validate the data before submitting it. This includes confirming that no input errors exist and verifying which fields are derived from other fields.

Note: The supervisor may want to provide key validation rules for EMIs to use prior to sending the data. If reporting is done via Excel sheets, the supervisor may consider providing templates with the necessary validation rules (formulas and further explanations) already built in.

9. Timeline for report implementation

The supervisor may want to specify the date reporting needs to begin and the cutoff date for the first reporting period. Consideration should be given to the need for EMIs to carry out any adaptations before they are able to report data with a minimum level of quality, such as system configurations. The supervisor should engage in specific consultations with EMIs to gauge the time the industry needs to begin reporting.

10. Standard definitions and format

EMIs are required to use the standard definitions and formats prescribed for each field, according to this guidance.

11. Questions

Questions about templates, standard definitions, and other topics related to R1–R4 should be directed to [*omitted in this anonymized version*].

12. Standard definitions of terminology used in reports

FUNDAMENTAL TERMINOLOGY		
Term	**Definition**	**Reports**
E-money account	An account opened by an EMI on behalf of a client. It may also be referred to as a "mobile money" or "mobile financial services" account.	R1, R3, R4
End user	The retail (individual) client who owns one or more e-money accounts and uses those accounts to make transactions and use other services. The term does not apply to corporate clients (e.g., agents, merchants, partners).	R1, R4
Total float	The sum of all balances in an EMI's registered e-money accounts, regardless of whether they are active, inactive, or dormant and regardless of account holder type (e.g., end user, agent, other). Total float is total outstanding e-money liabilities the EMI owes to all clients.	R1

OTHER TERMINOLOGY		
Term	**Definition**	**Reports**
Account balance	The closing balance of each e-money account registered in the e-money account system at the close of the reporting date. Account balance is the amount the EMI owes to each account holder.	R1
Accumulated loss with fraud and data security breaches	Loss accumulated with fraud and data security breaches includes not only direct loss of transaction value and reimbursements to clients but other costs that can be attributed to the fraud, such as administrative costs, costs in dealing with public authorities such as the police, legal costs, costs of fixing software or hardware, and estimated loss (e.g., clients who may have redeemed their balances or closed their accounts after a fraud incident). This value should be reported on a year-to-year basis, that is, accumulated loss in the year leading up to the reporting date.	R4
Active agent	An agent who has conducted at least one transaction in the last 60 days. If no transaction has been made in the past 60 days, the agent is considered inactive.	R1, R2
Active agent account	An e-money account owned by an active agent.	R1
Active end user and corporate account	E-money accounts owned by end users or corporates (except agents) in which at least one transaction has occurred in the last 90 days. Accounts with zero transactions within 90 days are considered inactive.	R1
Agent	A natural or legal person who has a direct agency relationship with an EMI based on an agent agreement.	R1, R2, R3
Airtime top-up	Purchase of airtime (mobile phone minutes) from mobile network operators (MNOs) by debiting an e-money account.	R3
Bank-to-e-money	Transfer from a bank account to an e-money account owned by the same client or another client.	R3
Bill payment	Payment to a biller such as a school or a landlord. Does not include utility payments, which are reported separately.	R3
Bulk transfer	Transfers typically made at the same time by a single payer entity to a large number of recipients. Examples include pension payments, salaries, and social transfers—both government-to-person (G2P) and business-to-person (B2P).	R3
Cash-in	A cash deposit that credits an e-money account ("loading" the e-money account).	R3

OTHER TERMINOLOGY		
Term	**Definition**	**Reports**
Cash-out	A cash withdrawal that debits an e-money account ("unloading" the e-money account). Cash-outs can happen at agents, bank branches, ATMs, POS, or other. When banking channels are used, this type of transaction does not include withdrawals from the client's bank account, even if the original funds came from an e-money account. Such transaction is classified as "e-money to bank transfer," and the withdrawal itself would be reported by banks in other payment statistics reports.	R3
Cash-in/cash-out at ATM, POS, and bank branches	Cash-in/cash-out (CICO) transactions using ATMs, bank branches, and POS, directly to/from an e-money account. (The e-money account system links with ATM, branch, or POS networks). Does not include deposits and withdrawals using a bank account.	R3
Confirmed fraud	A case of suspected fraud that has been confirmed and the EMI has acted upon.	R4
Data security breach	An incident in which sensitive, protected, or confidential data has been intentionally or unintentionally copied, transmitted, viewed, stolen, or used by an unauthorized party. It is the compromise of security that leads to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, protected data transmitted, stored, or otherwise processed (ISO/IEC 27040).	R4
Distributor	A company with which the EMI has a contract to distribute e-money to agents, among other responsibilities.	R2
Dormant agent account	An agent account that has remained inactive for the last six months.	R1
Dormant corporate or end user account	An account (except an agent account) that has remained inactive for the last 12 months.	R1
E-money account system	Often called a "mobile money platform," an account system (software) where client accounts, transactions, and balances are registered and managed.	R4
E-money-to-bank	Transfer from an e-money account to a bank account owned by the same client or another client.	R3
E-money-to-e-money "off us"	A peer-to-peer (P2P) transfer where the sender and receiver are end users who use their own e-money accounts at different EMIs. These are "interoperable transfers."	R3
E-money-to-e-money "on us"	A P2P transfer where the sender and receiver are end users of the same EMI.	R3
E-money-to-OTC	The sender's e-money account is debited but the receiver uses over the counter (OTC).	R3
External fraud	Fraud committed by end users or other parties external to an EMI's operations. May include clients using counterfeit cash, having unauthorized access to an agent's mobile phone or other transaction device, conducting fraud on web channels, using extortion, unlawfully repudiating funds or transactions, impersonating an agent or another client, refusing to return erroneous transfers, etc.	R4
Fraud	Fraud is a wrongful or criminal deception perpetrated by a person or corporate for unlawful or unfair personal or financial gain. Fraud may include a SIM card swap to the fraudster's SIM and other types of client or agent e-money account takeovers, phishing and social engineering leading to access to a client's or agent's data or account, agent asking for and using a client's personal identification number (PIN), agents charging clients unauthorized and excessive fees, fraudsters impersonating EMI staff, clients who are erroneously sent funds and refuse to refund them, withdrawal reversal fraud by clients, fake currency deposited by clients, and internal fraud (e.g., dummy accounts, access to client and suspense accounts, etc.).	R4
Fund safeguarding	Corresponds to the regulatory requirement for EMIs to safeguard total e-money float by placing an equivalent amount in trust account(s).	R1
Inactive account	An end user/corporate or agent account where no transaction has occurred in the last 90 days or 60 days, respectively.	None

OTHER TERMINOLOGY		
Term	**Definition**	**Reports**
Internal fraud	Fraud committed by staff, agents, or other parties (e.g., outsourced companies) with regular internal access to an EMI's operations. Examples include employees or agents defrauding the EMI by stealing unclaimed funds registered in temporary accounts, changing records and accounting, creating fictitious accounts and transactions, underreporting cash balances, etc.	R4
Inward remittance	P2P transfer sent into an e-money account from abroad through a partnership between the EMI and an institution abroad. An inward remittance is denominated in the local currency.	R3
Merchant	A commercial establishment, either physical or online, that accepts e-money transfers as a means of payment for goods or services. Some merchants may also be agents where clients conduct e-money-based transactions, such as withdrawals.	R2, R3
Nonprogrammed service disruption	Incident where the provision of e-money services is interrupted by a system outage or other cause. Includes system downtime due to internal or telecommunications failures. Reports should contain all system outages that last for more than one hour. A nonprogrammed service disruption does not include programmed downtime for maintenance purposes.	R4
Online merchant	A merchant that sells products and services on the internet, through an institutional website or a marketplace (e.g., Alibaba), and accepts e-money transfers as a means of payment for goods and services.	R2, R3
OTC	An over-the-counter (OTC) service an EMI provides to its clients. OTC occurs when a client sends or receives funds in cash without using their own e-money account. The sender, the recipient, or both may not use an account. In order to report OTC transactions, and for anti-money laundering/combating the financing of terrorism (AML/CFT) control purposes, EMIs must have special controls to identify OTC transfers and the clients who send or receive them.	R3
OTC-to-e-money	The sender uses OTC without debiting his/her account but the receiver's account is credited.	R3
OTC-to-OTC	Both the sender and receiver use OTC.	R3
Other corporate	Client owns one or more e-money accounts but is neither an individual end user nor an agent. In R1, "other corporate" includes merchants and distributors. In R2, merchants and distributors are reported separately.	R1, R2
Other payments to government	Payments to government authorities and entities, excluding government-owned utility companies, which are reported separately. Include taxes and fees.	R3
Payment to financial institution	A payment to a financial institution for the purpose of paying recurrent loan installments, credit card bills, and insurance premiums.	R3
Pending transaction	A transaction pending settlement. For instance, when a receiver has not cashed out an OTC transfer, the transfer is pending additional information from the client; a client has requested that a transfer be undone; a transaction is disputed by a client; a transaction is blocked pending further investigation, etc.	R4
Physical merchant	A merchant that sells products and services in physical stores and shops and accepts e-money transfers as a means of payment for goods and services.	R2, R3
Purchases and payments	Transfers related to the acquisition of goods and services offered by merchants, billers, utility companies, other government entities, and MNOs, as well as payments to financial institutions.	R3
Registered account	Includes any e-money account contained in the e-money account system.	R1, R2, R3, R4
Registered agent	All agents hired by an EMI, regardless of their activity status.	R2

OTHER TERMINOLOGY		
Term	**Definition**	**Reports**
Significant fraud	According to the EMI's own risk management methodology, a fraud incident placed high on the scale of significance for that particular type of incident. For the purpose of filling out R4, the EMI must list all confirmed fraud incidents placed in the two highest categories/levels of importance. The EMI must report a classification for each incident of fraud that specifies its position in the fraud classification system. For instance, if the EMI uses a classification system of 1 (critical) to 4 (less critical) and a fraud incident is classified as 1, such information must be provided in R4 under "significant fraud" (R4, fields 2.16–2.21). For each significant fraud, the EMI must report a description of the incident, losses incurred or estimated, and actions taken to repair the damage and avoid similar incidents in the future.	R4
Suspected fraud	A case where the EMI has flagged transactions for investigation under the suspicion of fraud by clients, agents, employees, or external parties. Transactions disputed by the end user or agent could become a suspected fraud, but this is not the only way the EMI may identify potential fraud. The EMI may have a fraud identification system that flags suspected transactions.	R4
Suspense account	Funds associated with pending transactions are placed in special temporary accounts that may be called virtual, settlement, temporary, or suspense accounts. These are to be reported in R4, field 1.3.	R4
Total transactions	The sum of all volumes and values of all types of transactions in the month, including any transaction type that may not be included in the template's tables. In such cases, the total may be greater than reported transaction types.	R3
Transaction disputed by end user or agent	Instance where the end user or agent contacts the EMI to request reversal or investigation of a transaction they claim has not been authorized or performed by them, or a transaction (e.g., a fee) the end user or agent believes is an error. Some disputed transactions become suspected or confirmed fraud.	R4
Trust account	A special type of bank account based on a trust agreement where an EMI deposits cash to back up the e-money float. The trust account must have a balance equal to or higher than the total e-money float at all times (updated at least daily by 4pm).	R1
Type of data security breach	EMIs must report both internal and external breaches and classify them by their level of seriousness.	R4
Utility payment	A payment to a government-owned or private utility company (e.g., water, electricity, gas, cable).	R3

13. Guidance for filling out reports

General guidance:

- Reports have accumulative fields (marked “stock data”) and fields requiring data about a change in the reporting period (marked “change data”). All account numbers and balances are to be reported as accumulative (stock) number/balance per the close of business on the reporting date, unless otherwise stated.
- Transaction volumes and values correspond to transactions conducted within the reporting period (“change data”), unless otherwise stated.
- For fields that permit more than one choice, it is not necessary to add a line for a category that has a null volume, value, or occurrence to report. Only categories with a reportable occurrence must be added.
- Some R4 fields require the description of single events, such as fraud, data security breaches, and nonprogrammed service disruptions. The EMI must report all incidents, adding as many rows as needed.
- Empty (blank) fields are not accepted.
- Currency values are denominated in [*omitted in this anonymized version*].
- Minimum value for numerical fields is zero.
- Negative values are not accepted in any numerical field.
- Open fields must be filled out.
- Monthly reporting should contain all reports and their respective tables. Incomplete reports will not be accepted.

R1. E-MONEY ACCOUNT NUMBERS AND BALANCES, AND TRUST ACCOUNTS		
Field	**Instruction**	**Format**
Table 1.1. Total e-money accounts		
1.1.	Number of e-money accounts registered in the account system	#.###
1.2.	Sum of balances in all accounts reported in 1.1.	$.$$$,$$
1.3.	Number of active e-money accounts	#.###
1.4.	Sum of balances in all accounts reported in 1.3.	$.$$$,$$
1.5.	Number of dormant e-money accounts	#.###
1.6.	Sum of balances in all accounts reported in 1.5.	$.$$$,$$
Table 1.2. E-money accounts: End user		
2.1.	Number of accounts registered by end users	#.###
2.2.	Sum of balances in all accounts reported in 2.1.	$.$$$,$$
2.3.	Number of active end user accounts	#.###
2.4.	Sum of balances in all accounts reported in 2.3.	$.$$$,$$
2.5.	Number of dormant end user accounts	#.###
2.6.	Sum of balances in all accounts reported in 2.5.	$.$$$,$$
Table 1.3. E-money accounts: Agents		
3.1.	Number of agent accounts	#.###
3.2.	Sum of balances in all accounts reported in 3.1.	$.$$$,$$
3.3.	Number of accounts of active agents	#.###
3.4.	Sum of balances in all accounts reported in 3.3.	$.$$$,$$
3.5.	Number of accounts by dormant agents	#.###
3.6.	Sum of balances in all accounts reported in 3.5.	$.$$$,$$
Table 1.4. E-money accounts: Other corporate		
4.1.	Number of corporate accounts, except agents	#.###
4.2.	Sum of balances in all accounts reported in 4.1.	$.$$$,$$
4.3.	Number of active corporate accounts, except agents	#.###
4.4.	Sum of balances in all accounts reported in 4.3.	$.$$$,$$
4.5.	Number of dormant corporate accounts, except agents	#.###
4.6.	Sum of balances in all accounts reported in 4.5.	$.$$$,$$
Table 1.5. Fund safeguarding/trust accounts		
5.1.	Select each bank where a trust account is held. Add a bank for each trust account and add as many rows as needed. If a bank holds more than one trust account, report each trust account in a different row, repeating the bank in field 5.1.	Bank name and code
5.2.	Total balance registered in each trust account, including interest	$.$$$,$$
5.3.	Total interest gains accumulated in each trust account	$.$$$,$$
5.4.	Sum of balances in all trust accounts reported in 5.2.	$.$$$,$$
5.5	Sum of accumulated interest in all trust accounts reported in 5.3.	$.$$$,$$
Table 1.6. Change in number of e-money accounts		
6.1.	Number of total e-money accounts opened in the reporting period	#.###
6.2.	Number of end user e-money accounts opened in the reporting period	#.###

R2. AGENTS, DISTRIBUTORS, AND MERCHANTS		
Field	**Instruction**	**Format**
Table 2.1. Agents		
1.1.	Total number of agents	#.###
1.2.	Total number of active agents	#.###
1.3.	Selection of each province where there are agents. Add as many rows as necessary to cover all provinces in which agents have been registered. Each province can only be chosen once.	Province name and code
1.4.	Total number of registered agents in the selected province	#.###
1.5.	Total number of active agents in the selected province	#.###
Table 2.2. Other corporate: Merchants and distributors		
2.1.	Total number of registered merchants	#.###
2.2.	Number of registered physical merchants	#.###
2.3.	Selection of each province where there are physical merchants. Add as many rows as necessary to cover all provinces in which physical merchants have been registered. Only one entry (row) is permitted per province.	Province name and code
2.4.	Number of physical merchants in the selected province	#.###
2.5.	Number of online merchants registered	#.###
2.6.	Number of distributors registered	#.###
Table 2.3. New agent appointments		
3.1	Total number of new agents appointed in the reporting period, regardless of their level of activity	#.###

R3. TRANSACTION VOLUMES AND VALUES		
Field	**Instruction**	**Format**
Table 3.1. Cash-in and cash-out		
1.1.	Total number of cash-in transactions in the month	#.###
1.2.	Sum of the value of all transactions reported in 1.1.	$.$$$,$$
1.3.	Number of cash-in transactions conducted at agents	#.###
1.4.	Sum of the value of all transactions reported in 1.3.	$.$$$,$$
1.5.	Number of cash-in transactions conducted at ATMs	#.###
1.6.	Sum of the value of all transactions reported in 1.5.	$.$$$,$$
1.7.	Number of cash-in transactions conducted at bank branches	#.###
1.8.	Sum of the value of all transactions reported in 1.7.	$.$$$,$$
1.9.	Total number of cash-out transactions in the month	#.###
1.10.	Sum of the value of all transactions reported in 1.9.	$.$$$,$$
1.11.	Number of cash-out transactions conducted at agents	#.###
1.12.	Sum of the value of all transactions reported in 1.11.	$.$$$,$$
1.13.	Number of cash-out transactions conducted at ATMs	#.###
1.14.	Sum of the value of all transactions reported in 1.13.	$.$$$,$$
1.15.	Number of cash-out transactions conducted at bank branches	#.###
1.16.	Sum of the value of all transactions reported in 1.15.	$.$$$,$$
Table 3.2. Transfers		
2.1.	Total number of transfers in the month	#.###
2.2.	Sum of the value of all transactions reported in 2.1.	$.$$$,$$
2.3.	Number of P2P e-money-to-e-money “on us” transfers	#.###
2.4.	Sum of the value of all transactions reported in 2.3.	$.$$$,$$
2.5.	Number of P2P e-money-to-e-money “off us” transfers	#.###
2.6.	Sum of the value of all transactions reported in 2.5.	$.$$$,$$

R3. TRANSACTION VOLUMES AND VALUES		
Field	**Instruction**	**Format**
2.7.	Number of e-money-to-bank transfers	#.###
2.8.	Sum of the value of all transactions reported in 2.7.	$.$$$,$$
2.9.	Number of bank-to-e-money transfers	#.###
2.10.	Sum of the value of all transactions reported in 2.9.	$.$$$,$$
2.11.	Number of bulk transfers	#.###
2.12.	Sum of the value of all transactions reported in 2.11.	$.$$$,$$
2.13.	Number of OTC-to-e-money transfers	#.###
2.14.	Sum of the value of all transactions reported in 2.13.	$.$$$,$$
2.15.	Number of OTC-to-OTC transfers	#.###
2.16.	Sum of the value of all transactions reported in 2.15.	$.$$$,$$
2.17.	Number of e-money-to-OTC transfers	#.###
2.18.	Sum of the value of all transactions reported in 2.17.	$.$$$,$$
Table 3.3. Purchases and payments		
3.1.	Total number of purchases and payments	#.###
3.2.	Sum of the value of all transactions reported in 3.1.	$.$$$,$$
3.3.	Number of bill payments, except airtime top-up and utilities	#.###
3.4.	Sum of the value of all transactions reported in 3.3.	$.$$$,$$
3.5.	Total number of airtime top-ups	#.###
3.6.	Sum of the value of all transactions reported in 3.5.	$.$$$,$$
3.7.	Total number of utility payments	#.###
3.8.	Sum of the value of all transactions reported in 3.7.	$.$$$,$$
3.9.	Total number of payments to government, except utility	#.###
3.10.	Sum of the value of all transactions reported in 3.9.	$.$$$,$$
3.11.	Total number of purchases at online merchants (e-commerce)	#.###
3.12.	Sum of the value of all transactions reported in 3.11.	$.$$$,$$
3.13.	Total number of purchases at physical merchants (in-store)	#.###
3.14.	Sum of the value of all transactions reported in 3.13.	$.$$$,$$
3.15.	Total number of payments to financial institutions	#.###
3.16.	Sum of the value of all transactions reported in 3.15.	$.$$$,$$
3.17.	Selection of each type of financial institution to which payments have been made in the month. Add as many rows as necessary. Only one entry (row) is permitted per type.	Name of institution type
3.18.	Number of payments to financial institutions	#.###
3.19.	Sum of the value of all transactions reported in 3.18.	$.$$$,$$
Table 3.4. Inward remittances		
4.1.	Total number of inward remittances	#.###
4.2.	Sum of the value of all transactions reported in 4.1.	$.$$$,$$
4.3.	Selection of each country from which inward remittances have been received in the month. Multiple selections allowed. Only one entry (row) is permitted per country.	Country name and code
4.4.	Number of inward remittance transactions for the selected country	#.###
4.5.	Sum of the value of all transactions reported in 4.4.	$.$$$,$$
Table 3.5. Total transactions		
5.1.	Total number of transactions conducted in the month. Include transaction types not included in the previous fields in R3, if any.	#.###
5.2.	Sum of the value of all transactions reported in 5.1.	$.$$$,$$

R4. RISK INCIDENTS		
Field	**Instruction**	**Format**
Table 4.1. Pending transactions and loss from fraud and data security breaches		
1.1.	Number of pending transactions as per close of reporting day	#.###
1.2.	Sum of the value of all transactions reported in 1.1.	$.$$$,$$
1.3.	Balance in all suspense accounts	$.$$$,$$
1.4.	The sum of incurred and estimated loss from fraud and data security incidents, as reported in Tables 4.2. and 4.3.	$.$$$,$$
Table 4.2. Fraud and data security breaches		
2.1.	Selection of the type of account in which transactions have been disputed and reported in 2.2.	"End user," "agent," or "other corporate" (drop-down menu)
2.2.	Number of transactions disputed by in the month, by type of account selected	#.###
2.3.	Sum of the value of all transactions reported in 2.2., by type of account selected	$.$$$,$$
2.4.	Total number of disputed transactions in the month, in all types of accounts	#.###,##
2.5.	Sum of the value of all transactions reported in 2.4.	$.$$$,$$
2.6.	Number of transactions flagged as potential fraud in the month, including cases already investigated and closed	#.###
2.7.	Sum of the value of all transactions reported in 2.6.	$.$$$,$$
2.8.	Total number of cases reported in 2.6. that have been confirmed as fraud	#.###
2.9.	Sum of the value of cases reported in 2.8.	$.$$$,$$
2.10.	Selection of the type of account for reporting of total number of confirmed fraud incidents. Multiple selections allowed. Only one entry allowed per selection.	"End user," "agent," or "other corporate"
2.11.	Number of transactions confirmed as fraud for the selected account type	#.###
2.12.	Sum of the value of the transactions reported in 2.11.	$.$$$,$$
2.13.	Selection of the source of confirmed fraud (internal or external). Multiple selections allowed. Only one entry allowed per selection.	"internal" or "external"
2.14.	Number of transactions confirmed as fraud, by source type	#.###
2.15.	Sum of the value of the transactions reported in 2.14.	$.$$$,$$
2.16.	Addition of row for each significant confirmed fraud in the month, as per its definition in this guidance. Add as many lines as necessary. All confirmed fraud incidents placed in the two highest categories/levels of importance—based on the EMI's fraud classification system—must be reported.	Entry number automatically generated
2.17.	Description of the level of significance for each significant fraud incident reported. For instance, if the EMI uses a 1 to 4 classification system and a fraud is classified at the highest level, e.g., 1 (critical), such information must be provided in this field.	Open field. Empty field not allowed
2.18.	Description of the significance scale used to classify fraud incidents	Open field. Empty field not allowed
2.19.	Description of each fraud incident	Open field. Empty field not allowed
2.20.	Number of e-money accounts affected in each fraud incident. If none, inform zero.	#.###
2.21.	Losses incurred and estimated for each incident	$.$$$,$$
2.22.	Description of actions taken to remediate the fraud incident and avoid similar occurrences in the future	Open field. Empty field not allowed
2.23.	Total number of data security breach incidents	#.###

R4. RISK INCIDENTS		
Field	**Instruction**	**Format**
2.24.	Addition of row for each data security breach reported. Add as many rows as needed.	Entry number automatically generated
2.25.	Date of each recorded data security breach incident. More than one incident permitted for the same date (in different rows).	dd.mm.yyyy
2.26.	Description of the type of each data security breach	Open text field. Empty field not allowed.
2.27.	Number of e-money accounts affected, if any, for each data security breach. If none, inform zero.	#.###
Table 4.3. Disruptions		
3.1.	Addition of row for each nonprogrammed service disruption incident of more than one hour. Add as many rows as needed.	Entry number automatically generated
3.2.	Date of each incident. More than one incident permitted for the same date (in different rows).	dd.mm.yyyy
3.3.	Start time of each incident	hh:mm (24-hour format)
3.4.	Total duration of each incident, from start time until service was reestablished for end users	#h#min
3.5.	Description of the cause of each incident	Open text field. Empty field not allowed.
3.6.	Actions taken related to remediate each incident and to avoid future similar incidents	Open text field. Empty field not allowed.