UNODC
United Nations Office on Drugs and Crime

MTS TRAINING COURSE

MANUAL

VIENNA - 2017

THE MANUAL HAS NOT BEEN FORMALLY EDITED.

CONTENTS

ACRONYMS AND DEFINITIONS

MTS or MTs	Money transfer services or Money transfers
MTS operator	A legal person licensed or registered by the competent authority to provide money transfer services, including through agents. This does not include Hawala and other similar service providers
Agent	A business entity or an individual who has direct partnership agreement with the MTS operator to provide money transfer services under the MTS operator's trademark
Master Agent	Is an Agent which is allowed to contract other agents (sub-agents) by the agreement with the MTS operator
Sub-Agent	Is a business entity or an individual (sub-)contracted by a Master Agent to provide money transfer services under the MTS operator's trademark
MTS providers	Includes both MTS operators and the Agents (Master Agents, Sub-agents)
KYC/CDD	Know Your Customer / Customer Due Diligence
KYA/ADD	Know Your Agent / Agent Due Diligence
DOB	Date of birth
COB	Country of birth
PEP	Politically Exposed Person
ATM	Automated teller machine
SSK/SST	Self-service kiosk / Self-service terminal
POS	Point of sale
FLA	Front-line associate – an employee of a MTS provider charged with servicing the customers at a point of sale
LEA	Law Enforcement Authority
FIU	Financial Intelligence Unit

CATEGORISATION OF MONEY TRANSFERS

1. Depending on the *funding source*, MTs can be categorized as follows:

   1.1. **Retail money transfer** is an in-person MT performed at a point of sale.

   1.2. **Account-based money transfer (ABMT)** is a money transfer received to or sent from the customer's bank account opened with an agent (bank). ABMTs can be performed through: (i) on-line banking, (ii) ATM and SST/SSK, (iii) ABMT-mobile application, or (iv) a phone call to the MTS operator's / the agent's call-center.

   1.3. **On-line (web-based) money transfer** is a money transfer received or sent from the customer's bank account (to a credit/debit card) via a specialized web-site which is maintained and operated either by the MTS operator, or by its agent, or by a third party contracted by the MTS operator. Unlike ABMT, the customer's bank does not necessarily need to be an MTS operator's agent.

   1.4. **Direct-to-bank money transfer (D2B)** can be sent through the MTS operator web-site or an agent's point of sale, but can only be received in the customer's bank account.

   1.5. **Mobile money transfer** is a money transfer received or sent from the mobile network customer's wallet associated with his/her mobile phone number.

   1.6. Money transfer to a **pre-paid card**.

2. Depending on *the parties involved in the transaction*, MTs can be categorized as follows:

   2.1. **Person-to-Person (P2P) money transfer**. Money is sent by an individual and paid to an individual, usually at an MTS operator's or an agent's location, and often in cash. Alternatively, money can be sent or paid directly from/to an individual's bank account, pre-paid card, or used for a money order.

   2.2. **Person-to-Business** & **Business-to-Person (P2B** & **B2P)**:

      (i) money transfer made by an individual to a business entity (e.g., education fees, utilities, mortgage fees, payments for public institution services, etc.);

      (ii) money transfer from a public institution or commercial entity to an individual (salary, pension, donation, etc.).

   These payments can be performed in the form of retail MTs, ABMTs, mobile MTs, etc.

   Similarly, there are a number of ways to receive the money: in cash at a MTS operator's or an agent's POS, to the customer's bank account, pre-paid card, or in the form of a check, etc.

   Descriptions of the business solutions offered by some MTS operators can be found at

their official websites[1].

2.3. **Business-to-Business (B2B) money transfers**:

(i) direct services provided to commercial customers. These can be used, for example, to settle international invoices (e.g. for imported goods), etc.

(ii) outsourcing services to customers which are financial institutions. These are intermediary services used to process back-office / back-end payments.

ML/TF RISKS ASSOCIATED WITH MONEY TRANSFERS

1. **Customer risks** – the risks posed by customers.

   For the customer risk monitoring and assessment, the following factors can be taken into account:

   - customer's transaction patterns are inconsistent with his/her business profile or financial standing, e.g.: (i) young people (e.g., students) making large, regular transactions;
   - customer's MT activity makes no economic sense or cannot be reasonably explained (with respect to MT purpose, funding sources, customer's relationship with payees/payers);
   - MTs take place in corridors involving high-risk jurisdictions;
   - customers transacting on behalf of a third party;
   - customers serviced remotely, whose identity arouse suspicion and/or is hard to verify (for example, customers making ABMTs and who struggle with providing details for identity verification);
   - customer's average MT amount significantly differs from an average MT amount;
   - customer presenting ID that appear to be falsified or altered;
   - customer whose MTs are subject to regular AML/CFT reporting;
   - customer sending MTs shortly after the receipt;
   - customer sending/ receiving MTs in even and/or high principal amounts;
   - customer receiving/ sending MTs from/to multiple senders/ payees, with no apparent family relationship between them.

2. **Agent risks** are the risks posed by MTS operator's agents (including Master Agents and Sub-Agents).

   The following factors can be considered for the agent risk analysis:

[1] http://business.westernunion.com
http://corporate.moneygram.com/products-and-services

- agent is located in a high risk jurisdiction or serves high-risk customers or transactions;
- agent is the subject of negative attention from credible media or law enforcement sanctions;
- agent operates AML/CFT compliance programs that do not effectively manage compliance with internal policies, monetary limits, applicable legal regulation, etc., or the AML/CFT compliance program implementation (in particular, transaction monitoring and reporting, record keeping, training, etc.) is inadequate;
- agent with a history of regulatory non-compliance and that is unwilling to follow compliance program review recommendations, and is therefore subject to probation, suspension or termination.

Depending on the agent's business model (e.g., non-banking entities like retailers), other factors may also be taken into account.

3. **Product risks** are the risks associated with MT products / services.

   MTS provider should be mindful of the risks associated with existing and new or innovative products or services not specifically offered by the MTS operator, but that make use of the MTS operator's systems to deliver the product or service. In particular, MTS providers should pay attention to the following:

   - if a product or a service provides for simplified identification requirements or favors anonymity;
   - if a product or a service allows for high volume or no-limit MTs;
   - adequacy of identification and KYC procedures;
   - expected typical customer of the product / service, as well as level of risks associated with such customer;
   - if a product / service is supposed to be offered in high-risk areas, etc.

4. **Geographic risks** are the risks associated with specific country or jurisdiction.

   For the purposes of assessing geographic risks, the following factors can be considered:

   - jurisdictions identified by credible sources[2] as providing funding or any other support for terrorist activities, or that have designated terrorist organizations operating within their territory;
   - jurisdictions identified by credible sources as having a significant level of corruption or other criminal activity;
   - jurisdictions that are subject to international sanctions, embargos or similar measures;

[2] Credible sources are considered official lists and reports produced by global specialized organizations such as FATF and its regional bodies, the UN, GRECO, etc., or listings, reports and research produced by a Member State agency combating financial crime (e.g., OFAC).

- jurisdictions with weak governance, law enforcement or regulatory regimes.

MTS operators and their agents should avoid engaging with any business entity and customer, which poses an unmanageable level of ML/TF risks. Inability to manage ML/FT risks may result in essential reputational, financial, administrative, or criminal penalties applied to the MTS provider and its executives.

MTS OPERATOR AGENTS

Depending on a MTS operator's business model and the applicable regulations, an MTS operator may provide money transfer services directly and/or through its partners (commercial entities and/or individuals). In this case, the partner entities are referred to as **Agents**. Upon agreement with the MTS operator, Agents may underwrite their own partners to provide services under the MTS operator's trademark. The underwriting agent is then referred to as **Master Agent**, whereas the underwritten agents are called **Sub-Agents**.

Below are the most common types of business entities that enter into partnership with an MTS operator and provide MTS on its behalf.

- banks;
- non-banking financial institutions;
- post offices;
- retail networks & Individual retail service providers. Examples can be large multi-store chains, small-sized drugstores, bookshops, car services, food market traders, ticket offices, individual entrepreneurs, etc.
- mobile network operators (MNOs);
- integrators / aggregators (intermediaries) – commercial business entities which partner with MTS operators to make MTS available for customers in a modern and convenient way. Examples: QIWI[3], iBox, Electropay, and others.

[3] https://qiwi.com/settings/account/identification.action#how-to-simple

AML/CFT COMPLIANCE CONTROLS APPLIED BY MTS OPERATORS

1. **Pre-enrolment control** (initial Know Your Agent/Agent Due Diligence) – a comprehensive scrutiny of a prospective agent preceding the so-called onboarding.

   The key elements of the pre-enrolment control:

   (i) due diligence of the beneficiary owners and the controlling persons[4]

   (ii) background checks of the prospective agent, e.g. whether the prospective agent is licensed/registered by the relevant national supervisory authority to provide payment services, length of time in business, ownership structure, creditworthiness, financial viability, etc.[5]

   (iii) review of the prospective agent's AML/CFT compliance programme;

   (iv) collecting appropriate additional information to better understand the prospective agent's business, such as: past record of legal and regulatory compliance, expected nature and level of transactions and customer base, geographical exposure, etc.

> **Good practice:**
>
> Some MTS operators develop and maintain an up-to-date agent database for keeping records about all existing and former agents, as well as those entities whose due diligence review resulted in rejection of the partnership application.

2. **Agent oversight** (ongoing Know Your Agent/Agent Due Diligence) refers to the continuous monitoring of the agents' activity. The degree and nature of the agent monitoring depends on various factors such as:

   - products or services provided by the agent;
   - the agent's transaction volume;
   - AML/CFT controls utilized by the agent (manual, automated or combination of both) and the adequacy of such controls;

[4] Can include checks against Consolidated United Nations Security Council Sanctions List, Office of Foreign Assets Control (OFAC) lists, EU terrorist lists, "PEPs"-databases, and other applicable domestic, regional and international sanctions and embargo lists. If required by local law, additional due diligence requirements may apply, for example, police clearance certificates for beneficial owners and controlling persons, or bankruptcy/insolvency checks, etc.

[5] This exercise may be performed either by the MTS operator (usually by a specifically designated unit) or by a third-party professional vendor such as Accuity, LexisNexis, FinScan, Thomson Reuters, EastNets and others.

- the agent's location (soundness of the AML/CFT regime in the country of the agent's registration);
- geographic reach of the agent's services (risks posed by the countries where the funds are sent or received);
- outcomes of previous agent's monitoring;
- public sources of information (regulatory reports, audit reports, etc.);
- adverse mass media information about the agent, etc.

Examples of enhanced due diligence measures that can be applied to high-risk agents:

(i) enhanced examination of the agent's transaction history and data integrity;
(ii) obtaining and evaluating the agent's explanation about suspicious behaviour;
(iii) confidential sampling of the questioned aspects of the agent's services ("mystery shopping");
(iv) on-site and off-site inspections.

3. **Audit.** MTS operators and their agents should have an independent audit function to test their AML/CFT programme with a view to establishing its effectiveness and the quality of the risk management across operations, departments, branches and subsidiaries, both domestically and, where applicable, abroad.

   The audit should be conducted by an internal audit unit that is not involved in the AML/CFT programme implementation or business operations of the MTS provider. This should also be enhanced by an audit conducted by an external qualified party such as PWC, Deloitte, EY, KPMG, Grand Thornton UK, and others.

4. **Transactions monitoring** refers to the continuous scrutiny of transactions to determine whether the transactions are consistent with the MTS operator's / agent's information about the customer(s) and the nature and purpose of the business relationship.

   There is no mandatory requirement to monitor transactions using sophisticated IT tools. However, for MTS providers that have large volumes of transactions, specialized software enabling an automated detection of suspicious MTs, may be the only realistic method of transaction monitoring. MTS operator agents may also face difficulties in monitoring the MTs performed by them (usually, when they act in a sub-agent capacity). In this case, MTS operator's support is crucial.

   Monitoring and identifying suspicious transaction activities (either automated or manual) is an extremely important tool for compiling a customer's risk profile and taking decision on application of enhanced CDD measures. More broadly, it seeks to support MTS providers in their decision making process of whether to enter into, continue or terminate the business

relationship with the customer. Transaction monitoring is based on pre-set combinations of various conditions which, when put together in specific scenarios, can expose high risks associated with the transactions and the behaviour of a customer.

Good practice:

Some MTS operators provide their agents with an automated tool for the monitoring of MTs, running reports and extracting information in a structured and straightforward way.

Suspicious customer activity can also be established by an FLA when meeting with a customer at an agent's POS. Therefore, an FLAs' cognizance with red-flag indicators as well as due vigilance is an effective tool for preventing abuse of MTS for illegal purposes (please refer to the Annex 6).

5. **Compliance data collection** and **data quality control** seeks to ensure the integrity and completeness of customers' and transactions' details that are entered in the operational system of the MTS operator.

   Either to send or to receive a MT, money transfer and customer related details should be collected and entered in the operational system of the MTS operator. To that end, the MTS operator should develop and implement a data collection template. A data collection template contains mandatory fields (e.g. transaction reference number, customer's name, customer ID or customer's address, customer's date and place of birth, etc.) and optional fields (e.g. customer's occupation, resident status, phone number, etc.). If mandatory fields are not filled out, the MT cannot be processed.

   The set of mandatory and optional details is not fixed. It differs depending on the nature of the MTS, the associated risks, as well as the local regulations governing these types of MTS.

Good practice:

A useful tool both for the agents' FLAs and compliance staff is a database developed and implemented by the MTS operator, which gives an overview of the MTS available / not available at any location and in any country where the MTS operator operates (directly or through agents). At a minimum, such a database should contain the following information:

- currencies available for sending and paying (in all countries and in all corridors);
- MT limits for outgoing and incoming transactions (in all countries and in all corridors);
- sending and payout restrictions, specifics and requirements (to include AML/CFT controls);
- agents' working hours, time zones, holidays and days-off in destination countries, etc.;
- list of acceptable ID (driver's license, national ID, passport, national insurance card, etc.) per country.

Good practice:

Data collection templates may have advanced functionalities such as pop-up screens, for example, for capturing additional information on high-risk customers or in higher risk situations. Such a functionality ensures mandatory collection of additional customer or transaction related information in a convenient and user-friendly way.

Quality and integrity of the collected data should be secured through the enforcement of specific rules such as (i) rejection of apparently false entries, for example, AAAAAA, 123456, $%^#@; (ii) (language-to-language) transliteration rules used to record customers' names in a holistic way.

In addition to this, MTS operators should develop instructions for their agents' FLAs on the processing of MTs, on introducing changes to MTs which have been sent but not paid out yet (substantial changes such as beneficiary's name), etc. (please refer to the Annex 2).

6. **Transaction limits**. Transaction limits can be either prescribed by the national regulations or applied by the MTS operator with a view of mitigation of high ML/TF risks associated with customers, channels, products, locations or corridors.

   Most common types of transition limits:

   - single transaction limit is the maximum allowed amount that can be transferred / received in a single transaction;
   - daily limit is the maximum aggregated amount that can be transferred / received over a business day (applicable to customers, an agent, agent location). It can be applied in combination with other limits.

Transaction limits may trigger either 'full stop', or request additional information.

7. **Real-Time Risk Analysis Control (RTRAC)** is the tool that combines various controls into a coherent and cohesive solution with a number of functionalities.

   Some examples of RTRACs:

   (i) a customer in Country "A" may receive max. 5 MTs per week from any number of customers in Country "B";
   (ii) a customer in Country "A" may receive any number of MTs for a total amount not exceeding 7K USD per week, from max. 5 different senders located in not more than 3 different countries;
   (iii) a customer in Country "A" may send max. 10 MTs over 20 days to max. 5 receivers in Country "B"; the total amount of all MTs is limited to 7K USD per 10 days.

8. **Interdiction** of customers is a control seeking to prevent the abuse of MTS by bad customers. Interdicted customers are restricted from using any MTS offered by the MTS operator.

   There are 2 main reasons for placing customers on the interdiction list:

   (i) MTS operator or its agents identifies suspicious or unusual customer behaviour involving fraud, tax evasion, gaming, lottery scams, etc. In this case, interdiction can be applied both to a presumptive infringer and victim;

   (ii) there is a restraining order, court order or seizure warrant received from a law enforcement or other competent public agency.

   MTS operators should elaborate procedures for both customer interdiction and customer reinstatement.

9. **Sanctions control** is a tool for the screening of customers against applicable sanctions (national and international) and embargo lists. Sanctions are imposed by international organizations and national governments, and are supposed to restrict / prohibit financial dealings with sanctioned jurisdictions, entities and/or individuals (e.g., UN sanction lists, OFAC, national terrorist lists, etc.).

   Sanction list screening can be automated and manual (less efficient). It may be conducted by either MTS operators or their agents themselves, or can be delegated to professional third-party vendors such as Accuity, CSI, LexisNexis, EastNets, Oracle, etc.

10. **PEPs control**. In line with FATF Recommendation 12, MTS operators and their agents should be required, in addition to performing normal customer due diligence measures, to:

- have appropriate risk-management systems to determine whether the customer or the beneficial owner is a politically exposed person;
- obtain senior management approval for establishing (or continuing, for existing customers) such business relationships;
- take reasonable measures to establish the source of wealth and source of funds; and
- conduct enhanced ongoing monitoring of the business relationship.

MTS operators and their agents should take reasonable measures to determine whether a customer is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organisation. The requirements for all types of PEPs should also apply to family members or close associates of such PEPs (please refer to the Annex 3).

Identification of a customer as a PEP may be entrusted to a professional third-party vendor such as Accuity, CSI, LexisNexis, EastNets, Oracle etc.

11. **On-spot checks** and **inspections** are two other measures to verify the soundness of the agent's AML/CFT controls. It can be performed either in the form of "mystery shopping" or agreed upon in advance between the MTS operator and the agent.

12. **Fraud protection control** seeks to provide prevention and protection from fraud. An effective MTS provider's anti-fraud policy should address the following three elements:

(i) fraud monitoring & fraud mitigation:
- assessment of fraud risks and application of a targeted action;
- implementation of rules in the operating system for early fraud detection;
- suspension of MTs suspected of being made with fraud purposes;
- customer interdiction;
- IT security (firewalls, anti-virus software, operating application update, precautions to emails, FLA passwords and access control);
- fraud reporting to LEA(s) and regulator(s).

(ii) fraud awareness raising and outreach[6]:
- guidelines and hands-on manuals for agents (FLAs);
- training for agents' FLAs ("red flags", typologies (please refer to the Annex 4),

[6] Examples: (1) https://www.westernunion.com/us/en/fraudawareness/stop-fraud.html
(2) http://corporate.moneygram.com/compliance/fraud-prevention
(3) https://www.riamoneytransfer.com/about-ria/preventing-fraud
(4) https://international.sigue.com/legal/consumer-fraud-awareness

etc.);
- warnings and information labels on desk tops and SSK terminals;
- anti-fraud videos, leaflets and posters available at agents' locations;
- publicly available online anti-fraud resources, fraud reporting hot-lines, anti-fraud campaigns, etc.).

(iii) anti-fraud stakeholder cooperation:
- national, regional and global anti-fraud efforts and initiatives to educate people about fraud scams and help them to avoid falling victim to fraud. An example: ScamAwareness.org, a non-profit American organization, reachable at www.scamawareness.org.

SPECIFICS OF KNOW YOUR CUSTOMER (KYC) & CUSTOMER DUE DILIGENCE (CDD)

KYC/CDD is understood as the processes of identifying and verifying the customers' identity. KYC/CDD is applied:

(i) when first establishing business relations with a customer (initial KYC/CDD);
(ii) when a customer carries out occasional transactions above the applicable designated threshold;
(iii) when there are suspicions of ML/TF;
(iv) when there are doubts about the veracity or adequacy of previously obtained identification data.

According to the FATF Recommendation 16, MTS providers must collect and include with the wire transfer relevant originator and beneficiary information, and make sure this information remains with the wire transfer across the whole payment chain. This information should include:

(a) the name of the originator;
(b) the originator account number (if such an account is used to process the transaction);
(c) the originator's address, or national identity number, or customer identification number, or date and place of birth;
(d) the name of the beneficiary; and
(e) the beneficiary account number where such an account is used to process the transaction.

Countries where an MTS provider operates may opt for a "*de minimis* threshold" approach for cross-border wire transfers that are not higher than USD/EUR 1000, below which a reduced set of details can be collected:

(a) the name of the originator (no requirement for other details of the originator)
(b) the name of the beneficiary; and

(c) the unique transaction reference number or an account number for each (if applicable).

Such information does not need to be verified for accuracy, unless there is a suspicion of money-laundering or terrorist financing, in which case the MTS provider should verify the information pertaining to the customer. **Countries may, however, require that incoming cross-border wire transfers below the threshold contain required and accurate originator information**.

A minimal set of customer and money transfer related details that are to be collected will depend on applicable legal and regulatory requirements, type of product / service, transaction channel, and other factors.

Customer risk profiling is an important element of the KYC/CDD programme, and incudes judgment over the function of the following elements:

- the number of transactions performed by the customer;
- the transaction amounts (individual and aggregated);
- the number of 'pay' and 'receive' agents and agents' POSs visited by the customer; whereabouts of these POSs vs customer's place of residence;
- the number of money transfer services used by the customer;
- the number of and types of the customer's counterparties, including nature of the relationship between them;
- the number of countries (especially high-risk ones) the customer receives or sends money to;
- the number of IDs used by the customer, including justification of this;
- the number / rate of SAR/STR filed involving the customer;
- etc.

KYC/CDD also includes screening of customers' names against sanction lists (national and international), PEPs lists, and "bad customer" lists, if applicable.

The extent of KYC/CDD measures may be adjusted to the extent permitted or required by regulatory requirements, based on the risks associated with the customer. KYC/CDD should be increased when the risks are high (Enhanced Customer Due Diligence or ECDD applies), and may be simplified where the risks are low (please refer to the Annex 1).

COMPLIANCE COOPERATION BETWEEN MTS OPERATORS AND THEIR AGENTS

Cooperation between an MTS operator and its agent starts with initial **partner (or agent) due diligence** – the review of each other's legal and regulatory compliance history, review of financial statements, criminal background checks of the owners (beneficiaries) and controlling persons, etc.

The parties either may conduct ADD themselves or engage with well-known professional service

providers such as LexisNexis, VERIBANC, Dun&Bradstreet, or major credit reporting agencies.

If any of the counterparties is not satisfied with the results of the initial ADD, the relationship should not be established.

Recommendation:

An entity should not be considered reliable:

- if any of its controlling persons or beneficial owners is "black-listed";
- if a controlling person, beneficial owner or the entity itself has been convicted of or pleaded guilty to any serious crime including but not limited to money-laundering, terrorist financing or fraud;
- if due diligence review determines that the perspective partner has knowingly facilitated money-laundering, terrorist financing, or consumer fraud.

A due diligence process does not stop with the initial ADD. Due diligence should be continuously performed during the entire business relationship. This stage of compliance cooperation may be referred to as **ongoing oversight**.

Due to the specifics of MTS business, oversight of partner entities is primarily the concern of MTS operators rather than of their agents since these are the agents who provide MTS on behalf of MTS operators and not vice versa.

An agent's ability to effectively monitor and analyse the customers' transaction activity is important especially in those jurisdictions where MTS operators do not have reporting obligations. Through ongoing transaction monitoring, an MTS operator and its agents can identify:

- ✓ transaction spikes;
- ✓ customer networks and groupings;
- ✓ unusual use of MTS;
- ✓ national and regional MTS specifics;
- ✓ high risk corridors and countries;
- ✓ external and internal risk factors and high risk concentrations;
- ✓ new illicit transaction patterns and emerging trends,
- ✓ etc.

Good practice:

A good practice is when an MTS operator supports its agents with an IT tool for the monitoring of the customers' transactions. Alternatively, agents may be provided with a regular transaction history log that can be used for monitoring and analysis purposes.

When a concentration of suspicious activity at an agent's location is identified, such activity should be immediately stopped and investigated. It is strongly recommended that the MTS operator and its agents closely cooperate for the purposes of a comprehensive investigation of suspicious activity including the cases of employee potential complicity into criminal conduct.

Regular compliance review is another method of monitoring a partner's AML/CFT compliance. Review can, however, go beyond AML/CFT issues and also include fraud prevention. The review procedures are to be risk-based and country specific. Compliance review can be performed in the form of on-site visits, via telephone, or a web-based video interview, depending on the risks identified and geographic considerations. In case of substantial developments (e.g. fraud, negative news, LEA inquiry, regulatory authorities' information, etc.) an additional or/and an in-depth review may be appointed.

It should be noted that by default (usually it is set forth in an agent agreement), the MTS operator should review the AML/CFT compliance of Master Agents and independent Agents, whereas Master Agents are responsible for reviewing the Sub-Agents' compliance. In certain cases, when the risk so warrants, MTS operators may request the review of a Sub-Agent's compliance that can be jointly performed by the Master Agent and the MTS operator.

Deficiencies identified during the ongoing monitoring and regular compliance reviews should be communicated to the Agent (Sub-agent) along with recommended corrective actions. In extreme cases (e.g., the Agent is suspected of being complicit in money-laundering, terrorist financing or fraud), the MTS operator should impose additional AML/CFT controls, or put the Agent on probation or suspension, or terminate the relationship.

Where appropriate, the MTS operator can provide (additional) training as a deficiency corrective measure. The MTS operator should maintain AML/CFT compliance and fraud training programmes not only for its employees but also for its agents. Master Agents should ensure that the Sub-agents are trained and have a training programme. The training programme should include training for new employees (at a minimum, FLAs and compliance officers), as well as an ongoing training for the existing employees. Ongoing training is essential to ensure everyone is cognizant of new developments, ML/TF trends and techniques, and is equipped to discover and prevent illicit activities.

Similar to the compliance review, the training program should consider country-specific risks, as well as the legal and regulatory environment. Methods for delivering training vary and can include:

- ✓ in-person training;
- ✓ conferences and workshops;

- ✓ self-learning materials;
- ✓ conference calls;
- ✓ etc.

Good practice:

A good practice is when the MTS operator sets up an online resource through which its agents can have remote access to a variety of management, marketing, and training tools including risk assessment resource guidelines, typology research, and other useful information.

Agents should be required to prove to the MTS operator that their employees (at least FLAs and compliance officers) have completed the required training (e.g. by presenting training logs, certificates of training completion, electronic reports, retaining copies of the training materials, etc.).

There may occur situations where intervention of the MTS operator compliance officer in the agent's business processes is sought. Such cases can be, for instance, setting and/or modifying transaction limits (agent limit, daily limit), reviewing and rolling out new products and channels, introducing changes into the existing AML/CFT cooperation due to legislative changes, when customers experience difficulties or delays with sending/ receiving MTs because of applicable sanction controls, customer black-listing and delisting, etc.

Good practice:

- ❖ The MTS operator develops a manual for their agents' FLAs with a step-by-step script on how to proceed in typical predicaments which have an AML/CFT background.
- ❖ If the frequency of the agents' inquiries is high, the compliance cooperation may be enhanced by the MTS operator's 24/7 hotline.
- ❖ The MTS operator may put the agents' customers on the internal "stop list" (filters), if the agent reasonably believes those are high-risk persons.

COOPERATION WITH REGULATORY AUTHORITIES

Cooperation in AML/CFT matters between MTS operators, their agents and regulatory authorities is usually driven by the requirement about the MTS sector compliance with the AML/CFT provisions, and making sure the risks pertinent to the MTS sector are identified and duly mitigated (please refer to the Annexes 5 and 7).

Information that can be shared between MTS operators and their agents, and regulatory authorities may include:

- ML/TF risk assessment (research and guideline);
- typologies of how money launderers or terrorist financers misuse MTS;
- general feedback on STRs/SARs and other relevant reports;
- international sanction lists, national sanction lists, industry level "bad customer" lists;
- transaction related data.
- etc.

COOPERATION WITH FIU

The cooperation in AML/CFT matters between an MTS operator and its agents, and the FIU emanates from the obligation to report suspicious transactions and/or suspicious activity (please refer to the Annex 9). Reporting is mandatory for the MTS operator's agents that are reporting entities under the national law.

MTS operators, as financial institutions, also have monitoring and reporting obligations. However, these obligations may vary depending primarily on whether the MTS operator is a reporting entity under national law or not.

Fulfilment of the reporting obligation becomes less straightforward in the case when the MTS operator is not a reporting entity under the domestic law. MTS operators always communicate terrorist financing related transactions. However, may do this not directly but through their agents so that the agents can further communicate TF-related suspicions to the national FIU. This is rarely the case in the case of an individual transaction suspected of money-laundering. Instead of reporting individual transactions suspected of money laundering, MTS operators which are not reporting entities under domestic law, often opt for sending suspicious activity (SARs) reports that can cover sometimes thousands of suspicious transactions. Such SARs are comprehensive in scope and encompass sometimes several agent's locations, and often cover a considerable period, e.g. 3 – 6 months. Similarly, MTS operators usually sends SARs to their agents so that the agents can report the suspicious activities to the national FIUs. The challenge in this context is to check if the SARs have been indeed filed by the agent to the domestic FIU.

COOPERATION WITH LAW ENFORECEMENT AUTHORITIES

The cooperation between MTS operators and their agents with LEAs is primarily driven by the LEAs' need to access customer and transaction related data available to MTS operators and/or their agents.

Law enforcement authorities are usually well cognizant of the tools to request and retrieve information that given them by law. However, quite often situations can happen when the requested information cannot be provided due to the fact that, for example, there are no legitimate reasons to request it, or the requested entity does not have it, or when seemingly the easiest and the shortest way to get the required data proves to be lengthy and/or futile. Of the mentioned, probably the biggest challenge is to identify the right holder of the required information (please refer to the Annex 8) – sending agent, paying agent, intermediary, or MTS operator.

Nevertheless, MTS operators, even when they do not have direct reporting obligation, may be approachable and willing to cooperate.

Recommendation:

If you (are a LEA and) need to request customer or transaction related information:

1. Check who the holder of the required information is (MTS operator or its agent(s); domestic agent(s) or a foreign one(s).
2. If the required information is kept by a domestic agent, proceed as per the national law. Mind all options of getting information and all possible counterparts (please refer to the Chart 1 below).
3. If the required information is kept by a foreign agent (please refer to Chart 2 and 3 below):
   (a) check with your MTS operator's contact person, ask for advice;
   (b) solicit the domestic FIU to retrieve the required information from its foreign counterpart FIU, or
   (c) request the foreign FIU directly, or
   (d) request the foreign counterpart LEA, or
   (e) request the information directly from the MTS operator.

CHART 1. Supervisory, LEA and FIU powers to request information on the national level

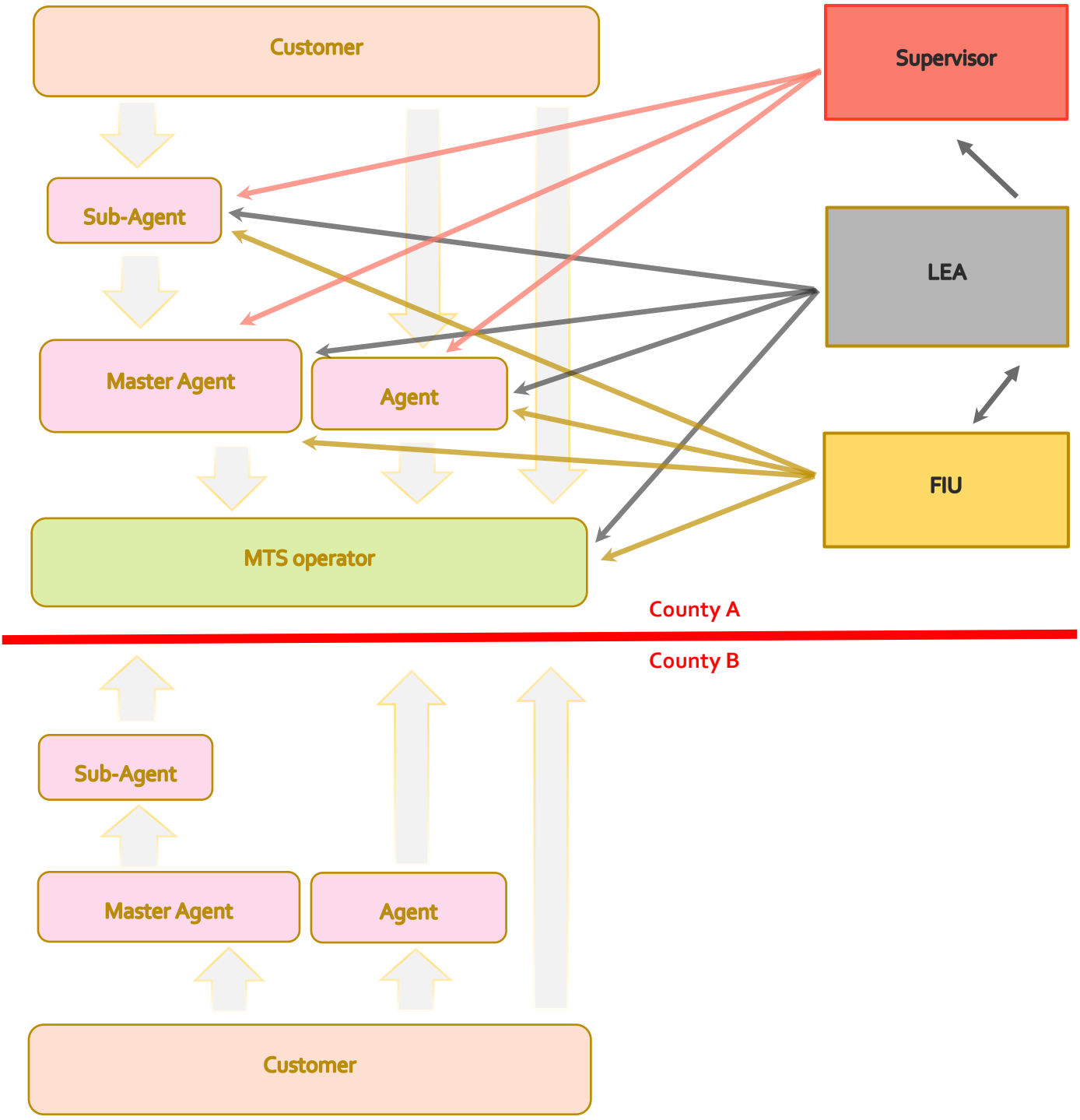


CHART 2. Supervisory, LEA and FIU powers to request information on the international level (scenario 1)

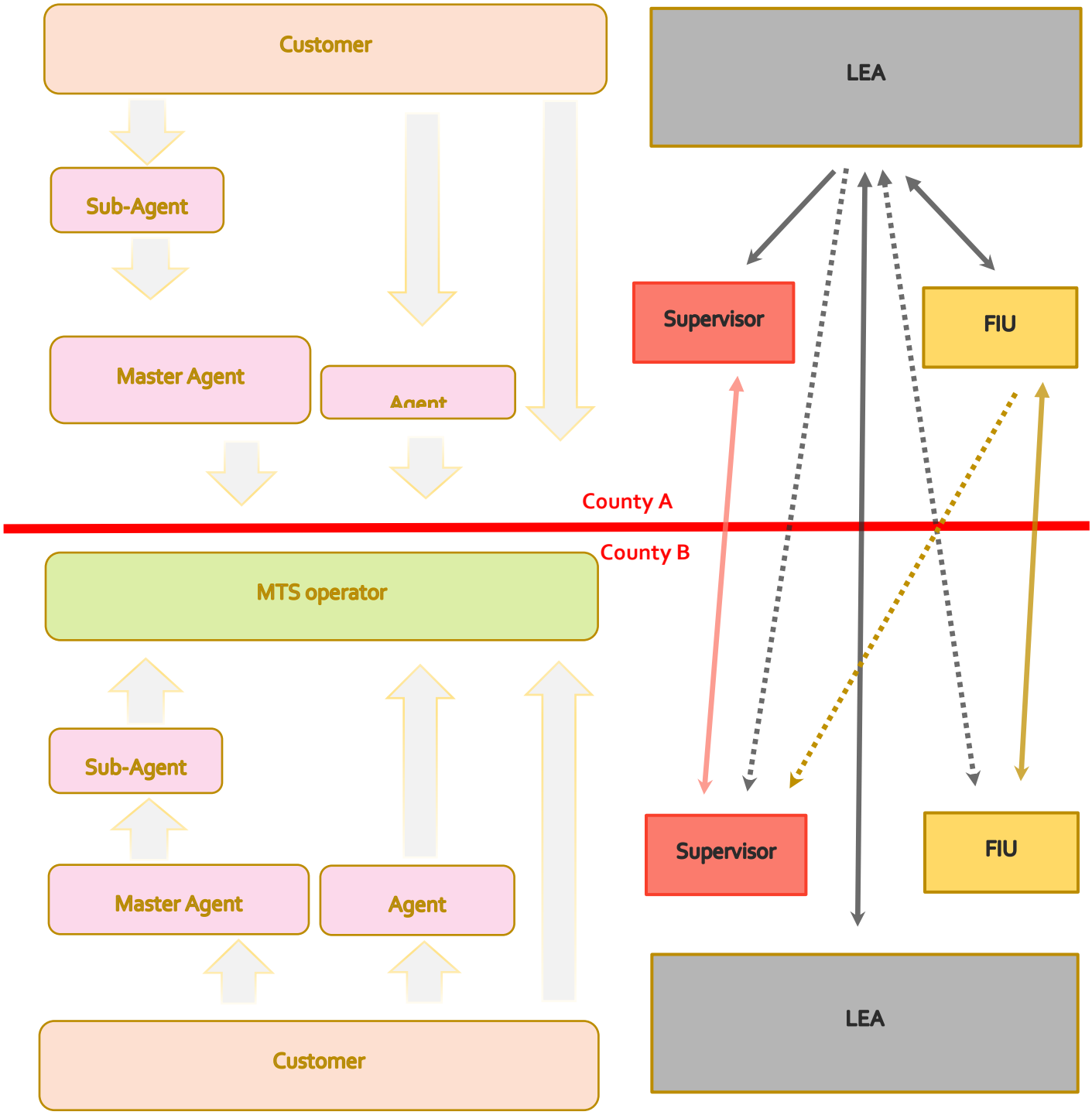
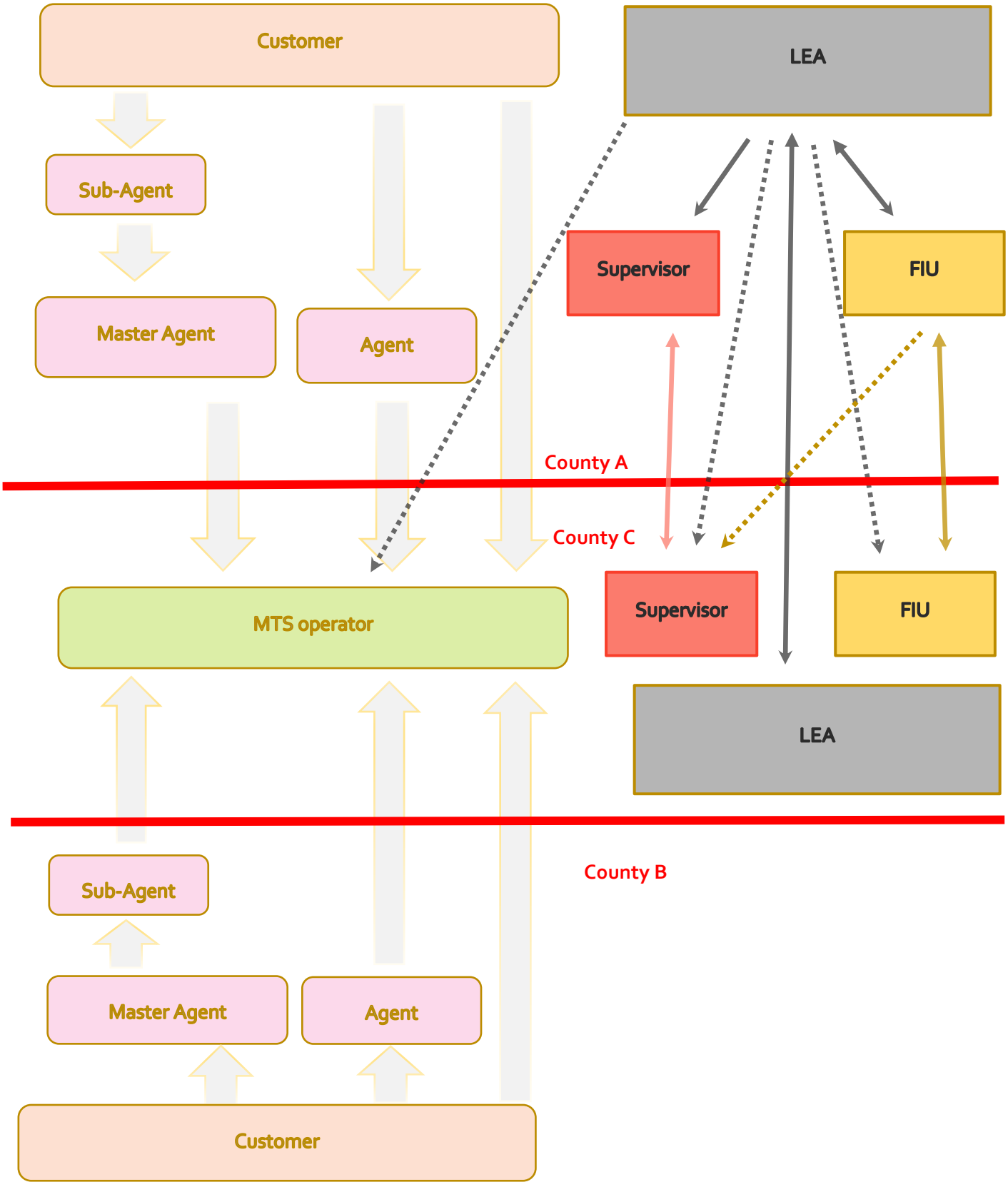


CHART 3. Supervisory, LEA and FIU powers to request information on the international level (scenario 2)



ANNEX 1. EXAMPLES OF ECDD AND SIMPLIFID CDD

ECDD will depend on the nature and severity of the risks. Thus, additional customer due diligence measures can take many forms.

Enhanced Customer Due Diligence:

- obtaining additional identifying information from a wider variety of or more robust sources;
- carrying out additional searches (e.g. verifiable adverse information searches via Internet);
- undertaking further verification procedures on the customer;
- verifying the source of funds or wealth involved in the transaction or business relationship;
- evaluating the information provided with regard to the destination of funds and the reasons for the transaction;
- seeking and verifying additional information from the customer about the purpose and intended nature of the transaction and/or the relationship with his/her counterparties.

Simplified Customer Due Diligence:

- obtaining fewer elements of customer identification data;
- less robust verification of the customer's identity;
- not collecting some specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship (but inferring the purpose and nature from the type of transactions or business relationship established);
- reducing the frequency of customer identification updates;
- reducing the degree and extent of ongoing monitoring and scrutiny of transactions.

ANNEX 2. SAMPLE INSTRUCTIONS FOR FLAs

- To pick up a MT, a customer (receiver) should provide:
  - a mandatory unique MT identifier number;
  - a valid ID;
  - the sender's name;
  - the originating country;
  - the expected amount (a reasonable tolerance range of 10% could be established);
  - an answer to a test question, if applicable;
  - a second valid ID, if applicable.

- Spelling mistakes should only be accepted if:
  - The spelling mistake does not change the gender of the first and second name (i.e. it does not change the name from female to male or vice versa. For example, changing Yevgeniy to Yevgeniya is not acceptable);
  - The misspelled name (first name/ last name) is common in the (local) spoken language(s). For example, changing the Russian name "Svetlana" to the Hungarian equivalent "Hajnalka" is not permissible;
  - The spelling mistake is not another valid name (the name does not change). For example, Michel cannot be changed to Michiel because those are different names, but Saasha can be changed to Sasha because the name is not changed);
  - The spelling mistake appears in only one of the following fields: (i) sender's first name, (ii) sender's last name, (iii) receiver's first name, (iv) receiver's last name.

ANNEX 3. PEPs CRITERIA

Anyone in any of the following roles should be considered a potential PEP:

(a) PEPs in government roles

- legislative bodies: a good example here would be a Member of Parliament;
- executive bodies: a PEP could be anyone from the head of state down to assistant ministers;
- diplomatic roles: ambassadors or charges d'affaires would be considered PEPs;
- judiciary bodies: key people working within supreme courts, constitutional courts or high-level judicial bodies;
- state-owned enterprises: a PEP would typically be anyone from a senior executive upwards. However, even former members of the board of directors no longer associated with an organisation may retain influence and still be flagged as PEPs.

(b) PEPs in organisations and institutions

- central financial institutions: examples here would be the Court of Auditors and members on the boards of central banks;
- armed forces: in this situation a PEP rating would typically only apply to a high-ranking officer;
- international sports committees: members of these committees may be influenced to vote on the location of major sporting events/contracts for building venues, etc., so have recently been included by FATF under their definition of a PEP.

(c) known 'close associates' who are considered PEPs

- anyone who has a close business relationship or joint beneficial ownership of legal entities or legal arrangements with a PEP;
- anyone who has the sole beneficial ownership of a legal entity which is known to have been set up for the benefit de facto of the PEP.

(d) immediate family members who are considered PEPs

- parents and children of PEPs;
- spouse or partner;
- siblings;
- uncles and aunts;
- even slightly indirect family members (such as in-laws) will be considered as a politically exposed person.

ANNEX 4. THE MOST COMMON FRAUD TYPOLOGIES[7]

1. **Disaster relief**
   In times of disaster, it is important to be aware of charity scams. There are many legitimate ways to provide support to help people impacted by floods, earthquakes, fires or other natural disasters. If you are eager to make a donation, give in a way that you have donated before or through a trusted organization or business where you fully understand how the funds are being collected and used. It is important to never send funds using a wire transfer service to someone you do not know.

2. **Relative in need**
   Did you receive a phone call from a grandchild or a family member? Or a "lawyer" or "police officer" representing your family member? Are they in despair because they have been detained in a faraway country for not having a fishing license or for catching a protected species of fish? Have they been in a car accident? Are they asking for money to pay fines or for car repair? Did a relative call because they need money for a family member in medical need or for medicine? This is a scam! Use precaution when sending money in any of these situations. These callers can request that you send money anywhere in the world. If you cannot verify with your family member (by calling their number you had before this call, not the "new number" the caller gives you) that they are requesting money and are not sure about the transaction, do not send the money. You will be out of pocket for any money that is sent.

3. **Elder abuse scam**
   A stranger begins a close relationship with you and offers to manage your finances and assets. Or, signatures on documents do not resemble your own signature. Do not get duped into parting with your money through financial abuse scams. Scammers will try to manipulate you into turning over property and/or money, and this can leave your cash, checking account or even life savings completely wiped out in one transaction. Financial abuse scams can take many forms, including telemarketing fraud, identity theft, predatory lending, and home improvement and estate planning scams. Never trust your money with anyone you do not know.

[7] Resources used (not exhaustive list):

(a) Federal Bureau of Investigation, Internet Crime Complaint Centre – https://www.ic3.gov/crimeschemes.aspx
(b) ScamAwareness.org is a non-profit organization dedicated to educating Americans about scams – http://www.scamawareness.org/
(c) Western Union https://www.westernunion.com/us/en/fraudawareness/fraud-types.html
(d) Money Gram http://corporate.moneygram.com/compliance/fraud-prevention/common-consumer-scams

4. **Lottery / sweepstakes**
   A victim gets an unsolicited phone call, email, letter or fax from someone claiming to work for a government agency or representing a well-known organization or celebrity, notifying them that they have won a considerable sum of money or a prize. The scammer gains their trust and explains that, in order to collect the winnings, they first have to send a small sum of money to pay for processing fees or taxes. Following these instructions, victims immediately wire the money, but never get their "winnings." And they are out the money they paid for "fees and taxes." Alternatively, victims get an unsolicited check or money order and directions to deposit the money, and immediately wire a portion of it back to cover processing fees or taxes. Weeks later, victims learn that the checks are counterfeit, but have already wired the money to cover the "taxes" and cannot get it back. And they have to pay their banks back for any money they withdrew.

5. **Buying a vehicle**
   Have you found a great vehicle online or in an advertisement with a price too good to be true? Are you being asked to send the down payment through a money transfer? Unfortunately, it is a scam. Do not send money for the vehicle to the seller or a payment representative. The vehicle purchase scammer may try to convince you to pay through a MTS provider to avoid sales tax and get a great price. They may even send you a letter or e-mail of authentication telling you that you have purchased the item, but in order to deliver it you need to wire funds first. You will not receive the car. Once money is wired and received, it cannot be recovered and, unfortunately, you will have lost any money transferred.

6. **Internet purchases**
   Have you found something online that interests you - a car, an apartment for rent or any item for sale? Does the price for the item seem to be too good to be true and are you being asked to pay for the item through a money transfer? Unfortunately, this is a scam. They may even send you a letter or e-mail of authentication telling you that you have purchased the item but need to wire funds first. Do not send the money. It is a scam. You will receive no merchandise. Once money is wired and received it cannot be recovered and unfortunately you will be out of pocket for any money transferred.

7. **Romance**
   The relationship scam starts simply: A man and woman meet on the Internet. The relationship progresses: They email, talk on the phone, and trade pictures. And, finally, they make plans to meet, and even to get married. As the relationship gets stronger, things start to change. The man asks the woman to wire him money; he needs bus fare to visit a sick uncle. The first wire transfer is small but the requests keep coming and growing – his daughter needs emergency surgery, he needs airfare to come for a visit, etc. The payback promises are empty; the money is gone, and so is he.

8. **Loans**
   Scammers pose as representatives from phony loan companies and use authentic-looking

documents, emails, and websites to appear legitimate. They charge "fees" in advance of making loans. Consumers pay, but the loans never come through. Scammers are long gone and they sometimes regularly change the name of their "businesses" to avoid law enforcement.

This is one variation of a scam called the "advance fee" or "prepayment" scam. Scammers can also lure victims in with promises of investments or inheritance gifts in exchange for a fee. But it all comes down to the same theme: Victims pay money to someone in anticipation of receiving something of greater value and then receive little or nothing in return.

9. **Overpayment**

With overpayment scams, fraudsters play the role of buyer and target consumers selling a service or product. The "buyer" sends the seller a legitimate-looking check, usually drawn on a well-known bank, for an amount higher than the agreed-upon price. They contact an explanation for this overpayment and instruct the seller to deposit the check and wire back the excess funds. Weeks later, the victim learns the check is fake, but is still obligated to pay the bank back for any money withdrawn.

10. Employment

Employment scams generally start with a too-good-to-be-true offer – to work from home and earn thousands of dollars a month, no experience needed – which end with consumers out of a 'job' and out of money. They generally follow one of three patterns:

(i) Scammers pose as a new 'employer' and send victims a check to cover up-front expenses, like supplies. Victims deposit the check, buy the necessary supplies and wire any remaining funds back to the scammer. Weeks later, they find out the checks are fake and they need to pay the entire amount.

(ii) Scammers pose as 'recruiters' pitching offers of guaranteed employment or as 'employers' extending job offers on the condition that victims pay up front for things like credit checks or application or recruitment fees. Victims pay, but job offers never materialize.

(iii) Scammers pose as 'company' representatives and seek sensitive personal and/or financial information from victims under the guise of doing credit or background checks. They then target victims later on for identity theft.

11. Anti-Virus

A fraudster contacts the victim claiming that they are from a well-known computer or software company and have detected a virus on the victim's PC. The fraudster advises that the virus can be removed for a small fee with a payment by either credit card or an online money transfer. The fraudster then requests remote access to the victim's computer to install anti-virus software to remove the virus. Unfortunately, the fraudster uses this access to take control of the victim's computer to install software and malware. The fraudster

may also steal credit card information that is on the computer and use it to complete online money transfer transactions.

12. **Mystery Shopping**
    Mystery shopping scams are popular with criminals who target employment websites. Scammers send victims a check and tell them to use the funds to "evaluate" an MTS operator's money transfer service. Victims wire the money only to find out later that the checks bounce and they are responsible for paying the bank back.

.

ANNEX 5. EFFICIENCY OF FULFILLING AML/CFT OBLIGATIONS BY DIFFERENT CATEGORIES OF AGENTS [8]

	Banks	**Non-banking financial institutions (NBFIs)**	**Post offices**	**Retail networks and individual retail service providers**	**Mobile network operators (MNOs)**	**Integrators / Intermediaries**
	Master Agent, Agent, Sub-Agent	Master Agent, Agent, Sub-Agent	Agent, Sub-agent	Agent, Sub-agent	Agent	Agent
(1) Compliance officer	Usually have strong compliance function and independent AML/CFT unit, including chief compliance officer, and often AML/CFT staff in field offices.	Sometimes the compliance officer performs additional functions, which are not related to AML/CFT (e.g. internal audit, security, etc.).	Compliance officer often performs additional functions which are not related to AML/CFT (e.g. internal audit, security, etc.).	In case of individual retailers, all functions (business, compliance, operations, etc.) are executed by the same person. In case of retail networks, compliance officer may be charged with other functions which are not related to AML/CFT (e.g. internal audit, security, etc.).	Compliance officer (if any) often performs additional functions which are not related to AML/CFT (e.g. internal audit, security, etc.).	Compliance officer (if any) often performs additional functions which are not related to AML/CFT (e.g. internal audit, security, etc.).
(2) KYC & CDD	Usually have well developed KYC/CDD policies and procedures which meet the industry-level standards, and are efficiently enforced.	Since NBFIs provide limited financial services, KYC/CDD may be less comprehensive	Adequacy and enforcement effectiveness of the KYC/CDD can be an issue.	KYC/CDD function is usually limited to customers' identification (with limited verification capacity) and keeping customers' ID records, often in paper form. KYC/CDD adequacy and its selectiveness can be a concern.	Usually have sufficient financial resources and may thus be able to duly fulfil KYC/CDD, including maintaining electronic customer database. However, KYC/CDD efficiency will be dependent on AML/CFT regulations in	Usually have sufficient financial resources and may thus be able to duly fulfil KYC/CDD, including maintaining electronic customer database. However, KYC/CDD efficiency will be dependent on AML/CFT regulations in place,

[8] This this an aggregated picture based on the subjective judgment. The situation can differ from jurisdiction to jurisdiction.

	Banks	Non-banking financial institutions (NBFIs)	Post offices	Retail networks and individual retail service providers	Mobile network operators (MNOs)	Integrators / Intermediaries
	Master Agent, Agent, Sub-Agent	Master Agent, Agent, Sub-Agent	Agent, Sub-agent	Agent, Sub-agent	Agent	Agent
					place, therefore may be selective or lacking comprehensiveness.	therefore may be selective or lacking comprehensiveness. .
(3) Monitoring	Usually have specifically designated team, sufficient resources, and efficient automated controls and tools to perform the monitoring	Monitoring is often performed manually which reduces its efficiency.	Monitoring is often performed manually which reduces its efficiency.	Monitoring is usually performed manually, which in combination with other factors such as lack of resources, adequate training and supervision, significantly reduces its efficiency.	Usually have adequate financial resources in order to maintain automated tools and instruments for monitoring, However, there is often a lack of AML/CFT regulations in respect of MNOs and, as a result, poor enforcement and lax supervision can be a serious challenge.	Usually have adequate financial resources in order to maintain automated tools and instruments for monitoring. However, there is often a lack AML/CFT regulations in respect to these types of entities, and, as a result, poor enforcement and lax supervision can be a serious challenge.
(4) Reporting	Usually have specifically designated team, sufficient resources, and efficient automated controls and tools to fulfil the reporting obligations	Often are able to efficiently fulfil reporting obligations. However, the reporting efficiency is heavily dependent on the level of supervision, the training adequacy and the availability of resources.	Often are able to efficiently fulfil reporting obligations. However, the reporting efficiency is heavily dependent on the level of supervision, the training adequacy and the availability of resources.	Similar to KYC/CDD, the reporting efficiency is usually poor due to the often lax supervision, lack of training and limited financial resources.	May have reporting obligations. However, the often lack of effective AML/CFT regulations and lax supervision results in inefficient reporting.	May have reporting obligations. However, a lack of effective AML/CFT regulations and lax supervision may by a serious concern.

	Banks	**Non-banking financial institutions (NBFIs)**	**Post offices**	**Retail networks and individual retail service providers**	**Mobile network operators (MNOs)**	**Integrators / Intermediaries**
	Master Agent, Agent, Sub-Agent	Master Agent, Agent, Sub-Agent	Agent, Sub-agent	Agent, Sub-agent	Agent	Agent
(5) Training	Usually have strong training programmes, and often industry level training centres and e-learning programmes.	Adequacy of training programmes and effectiveness of their implementation is usually dependent on the level of supervision and availability of resources. Thus, training programmes are not always sufficient.	Adequacy of training programmes and effectiveness of their implementation is usually dependent on the level of supervision and availability of resources. Thus, training programmes are not always sufficient.	Often lax AML/CFT regulations coupled with inadequate supervision and lacking financial & human resources result in occasional and often poor training.	Due to often lacking or vague AML/CFT regulations, training programmes (if any) are often developed based on a subjective understanding of the AML/CFT obligations.	Due to often lacking or vague AML/CFT regulations, training programmes (if any) are based on a subjective understanding of the AML/CFT obligations.

Interpretation of the colours assigned:

Level of efficiency	high	moderate	low

ANNEX 6. THE MOST COMMON TYPOLOGIES OF CRIMINAL CONDUCT INVOLVING THE MTS SECTOR

Below are the most common scenarios indicative of high risks associated with MTS. These are the most common typologies of criminal conduct in which MTS providers can be either knowingly or unknowingly involved. There is an explanation of each pattern, with the "red flags" and vigilance recommendations provided for FLAs and compliance officers.

I. Suspicious activity which can be indicative of money-laundering or other illicit/ prohibited activities and which *can be established through follow-up transaction analysis*:

Suspicious activity	Explanation & "red flags"	Examples
Higher principle customer	A single customer sending or receiving higher MT amounts compared to other customers (sender or receiver) at agent's location.	A single customer sending MTs totalling $15,000 in a single week when the average amount sent by other customers is about $500.
Higher frequency customer	A single customer sending or receiving a higher number of MTs (sent or received) compared to other customers at agent location.	A single customer receiving 20 MTs (regardless of amount) over a two-week period when the average number received by other customers is less than 3.
Many-to-One / One-to-Many	⇒ A single customer receiving at least two MTs from two or more different senders; there is no obvious familial relationship between senders and payees; ⇒ Multiple customers sending MTs to a single payee; there is no obvious familial relationship between senders and payees; ⇒ Customer sends multiple MTs, often in amounts below the reporting threshold, to multiple recipients, usually in different countries.	⇒ A single customer receiving multiple MTs from 15 senders (of various nationalities) from different countries. ⇒ 15 MTs sent in even amounts of $5 000 each by 5 customers from a single agent location to a single payee in another country; no apparent familial relation between senders and payees.

Suspicious activity	Explanation & "red flags"	Examples
Structuring & Avoidance of reporting / identification	⇒ Multiple customers who appear to be connected, send MTs to a common payee which are just a bit below the amount requiring any ID, and / or below the daily transaction limit; ⇒ A single customer sends multiple MTs, often in even and/or equal amounts, during a short period, to the same payee.	Assuming a $5 000 threshold: Customer sending three $4 999 MTs on the same day, often within minutes.
Blitz MTs	⇒ Multiple MTs sent on the same day, within minutes, by a single customer or multiple customers; often sent to a common payee and/or geographical region; ⇒ Multiple MTs received on the same day, within minutes to a single customer or multiple customers; often received from one or multiple geographical areas.	⇒ Four customers sending 12 MTs over 30 minutes to two payees who appear to be relatives. ⇒ Five customers receiving 20 MTs within one hour from multiple senders in 4 countries.
MTs flipping	Customer receives one or more MTs, which are then sent on to a different payee. Typically, MTs are sent for less than they were received; MTs may be sent to higher risk countries and/ or countries known for illicit activity.	Customer receives $5 000 from Austria and on the same day the same customer sends out $4,800 to a payee in China.

Suspicious activity	Explanation & "red flags"	Examples
Sending / Receiving from/to high-risk or unusual corridors	MTs being sent to or received from higher risk countries or through unusual corridors.	Customer sending/receiving MTs to and/or from higher risk countries.
Customer data integrity	⇒ Personal details of the customer appear to be invalid; ⇒ Personal details of the customer are entered in consecutive order or in sequence; ⇒ Multiple customers with common biographical data; ⇒ A single customer with inconsistent / various biographical information entered for multiple MTs.	⇒ Customer "A" has a phone number of 111-222-3333 or an address of "Another World"; ⇒ Customers "A", "B" and "C" have the following phone numbers: 11-11-112; 11-11-113; 11-11-114; ⇒ Customers "A", "B" and "C" have passport number 123321 entered for their ID number; ⇒ Customer "A" has two or more different passport numbers or the passport numbers differ by just a single character; ⇒ Customer "A" regularly transacts at the location but each time gives another address.
Potential agent's (FLA) complicity	⇒ Number of irregular FLA transaction look-up patterns known as "surfing".	⇒ MTs have been regularly checked by the FLA but not paid out; ⇒ MTs have been regularly checked during the day(s) preceding the day of pay out.

II. Suspicious activity which can be indicative of money-laundering or other illicit / prohibited activities, and which *can be identified by FLAs at a point of sale*:

Suspicious activity	Explanation & Red Flags	Recommendations for FLAs
High frequency transactions	⇒ Customer sends or receives multiple, sometimes small amount MTs in a short period of time; many or all of the MTs are in even amounts; ⇒ Customer makes multiple MTs in small amounts in a short period of time payable to the same person or a group of related persons; ⇒ Customer purchases multiple prepaid cards or gift cards in small amounts in a short period of time; ⇒ Customer comes many times a day to conduct MTs when he/she could have completed them all the first time he/she came in.	⇒ In case of suspicions, ask the customer questions to ascertain: - the source of the money, - the purpose of the MT, - the relationship between the customer and the recipient. ⇒ Consult your supervisor to ascertain whether you should proceed with the MT. ⇒ Notify the MTS operator's compliance officer. ⇒ Report the MT (attempt) to FIU (if applicable).
MT flipping	Customer receives MTs and then immediately attempts to send one or more MTs using the funds from the previous transaction; the customer might explain that he/she is doing this for a job.	⇒ In case of suspicions, ask the customer questions to ascertain: - the source of the money, - the purpose of the MT, - the relationship between the customer and the recipient. ⇒ Consult your supervisor to ascertain whether you should proceed with the MT. ⇒ Notify the MTS operator's compliance officer. ⇒ Report the MT (attempt) to FIU (if applicable).

Suspicious activity	Explanation & Red Flags	Recommendations for FLAs
One-to-Many / Many-to-One	⇒ Customer sends multiple, usually small amount MTs at a time to different recipients; the recipients may be connected (e.g., the same family name), but not necessarily; ⇒ A single customer receives multiple MTs from different senders without plausible justification of a business or personal relationship between them.	⇒ In case of suspicions, ask the customer questions to ascertain: - the source of the money, - the purpose of the MT, - the relationship between the customer and the recipient. ⇒ Consult your supervisor to ascertain whether you should proceed with the MT. ⇒ Notify the MTS operator's compliance officer. ⇒ Report the MT (attempt) to FIU (if applicable).
Customer data integrity	⇒ Customer uses a fake ID, or different IDs on different occasions (name, address, or identification number may be different); ⇒ Two or more customers use the same or similar ID (photo or name may be different); ⇒ Customer changes or cancels a MT after learning that he / she must show ID.	⇒ In case of suspicions, ask the customer questions to ascertain: - the source of the money, - the purpose of the MT, - the relationship between the customer and the recipient. ⇒ Consult your supervisor to ascertain whether you should proceed with the MT. ⇒ Notify the MTS operator's compliance officer. ⇒ Report the MT (attempt) to FIU (if applicable).

Suspicious activity	Explanation & Red Flags	Recommendations for FLAs
Overall suspicious customer behaviour	⇒ Customer is in a hurry, nervous, evasive, aggressive or uncooperative; ⇒ Customer is reluctant to provide ID or information; ⇒ Customer appears only at the location opening, closing or peak times; ⇒ Customer tries to impress FLA with his/her substantial future business or wealth; ⇒ Customer offers a tip, bribe or other inappropriate gift; ⇒ Customer has been the subject of a law enforcement inquiry; ⇒ Customer provides inconsistent information when asked questions; ⇒ Customer comes several times in one day to conduct transactions that are just below the reporting threshold; ⇒ Customer is not concerned about price or is too familiar with the reporting rules; ⇒ Multiple customers appear to know each other outside the premises, but ignore each other while they are inside the location.	⇒ In case of suspicions, ask the customer questions to ascertain: - the source of the money, - the purpose of the MT, - the relationship between the customer and the recipient. ⇒ Consult your supervisor to ascertain whether you should proceed with the MT. ⇒ Notify the MTS operator's compliance officer. ⇒ Report the MT (attempt) to the FIU (if applicable).

III. The most common typologies of a criminal conduct in which MTS providers can be knowingly or unknowingly involved:

Criminal activity	Explanation & Red Flags	Recommendations for FLAs
Trade in counterfeit goods	⇒ Customer works in a retail company (typically one selling clothes, electronics, etc.) and sends MTs to individuals or companies in countries known as manufactures of counterfeited goods; ⇒ Customer provides inconsistent information (e.g., he/she sells expensive goods, but cannot give a business address); ⇒ Customer says he/she can give you a "good deal" or a "great price" on products and through conversation, you determine that the goods are likely counterfeit.	⇒ In case of suspicions, ask the customer questions to ascertain: - the source of the money, - the purpose of the MT, - the relationship between the customer and the recipient. ⇒ Consult your supervisor and/or compliance officer to ascertain whether you should proceed with the MT; ⇒ Notify the MTS operator's compliance officer; ⇒ Report the MT (attempt) to the FIU (if applicable).
Human trafficking & human smuggling	Customer appears to be controlled by someone else (controller): ⇒ may be nervous or reluctant to answer questions about the MT; ⇒ is not able to speak, controller speaks for him/her, but puts the MT in the customer's name; ⇒ does not hold his/her own ID, controller holds it for him/her. ⇒ has bruises or other signs of physical abuse; ⇒ picks up the MT and immediately hands it to the controller; ⇒ brings in a completed MT form in someone else's	⇒ In case of suspicions, ask the customer questions to ascertain: - the source of the money, - the purpose of the MT, - the relationship between the customer and the recipient. ⇒ Consult your supervisor and/or compliance officer to ascertain whether you should proceed with the MT; ⇒ Notify the MTS operator's compliance officer; ⇒ Report the MT (attempt) to the FIU (if applicable).

Criminal activity	Explanation & Red Flags	Recommendations for FLAs
	handwriting; ⇒ does not speak the local language; ⇒ cannot give his/her name and address without reading them from the MT form. In addition, MTs performed by such customers may have the following features: ⇒ are split in several small, even amounts of cash; ⇒ are just below the reporting limit; ⇒ include bribes, tips, or threats to the FLA (to facilitate the MT); ⇒ involve the customer receiving multiple MTs from different senders in a short amount of time (many-to-one); ⇒ involve multiple customers sending transactions to the same receiver in a short amount of time (one-to-may); ⇒ involve unrelated customers who provide the same address or phone number (data integrity); ⇒ the customer does not have a local address but appears to live close by because he/she is a frequent customer; ⇒ the customer is deliberately changing the spelling of his/her name for different MTs.	

Criminal activity	Explanation & Red Flags	Recommendations for FLAs
Trade in counterfeited drugs	⇒ Customer's behaviour or comments are indicative of the money being used for, or linked to, illegal drug sales; ⇒ When asked about the MT, the customer mentions some of the drugs names; ⇒ The recipient of the MT is a name that appears to be a pharmaceutical company; ⇒ Customer may be nervous or reluctant to answer questions about the MT; ⇒ Customer conducts regular MTs to / from countries associated with sales of illegal drugs, such as Brazil, China, Costa Rica, India, Mexico, and Pakistan.	⇒ In case of suspicions, ask the customer questions to ascertain: - the source of the money, - the purpose of the MT, - the relationship between the customer and the recipient. ⇒ Consult your supervisor and/or compliance officer to ascertain whether you should proceed with the MT; ⇒ Notify the MTS operator's compliance officer; Report the MT (attempt) to the FIU (if applicable).
Tax evasion	⇒ Customer uses large amounts of money to conduct MTs instead of wiring the money from a bank account; ⇒ Customer shows signs of a wealthy lifestyle without any apparent job or source of income that would support such a lifestyle; ⇒ Customer uses currency to send MTs to pay for goods.	⇒ In case of suspicions, ask the customer questions to ascertain: - the source of the money, - the purpose of the MT, - the relationship between the customer and the recipient. ⇒ Consult your supervisor and/or compliance officer to ascertain whether you should proceed with the MT; ⇒ Notify the MTS operator's compliance officer; Report the MT (attempt) to the FIU (if applicable).

Criminal activity	Explanation & Red Flags	Recommendations for FLAs
Terrorist financing	⇒ MTs occur to or from a higher-risk geographic location without an apparent plausible reason, or the activity is inconsistent with the customer's business or profile; ⇒ Many small incoming MTs are received, whereupon all or most of the MTs are wired to another country almost immediately in a way inconsistent with the customer's business or profile; ⇒ Customer is reluctant to provide ID or to answer questions about the MT; ⇒ Customer tries to persuade an FLA not to file required reports or maintain required records; ⇒ Customer asks to be exempted from reporting or record keeping requirements.	⇒ In case of suspicions, ask the customer questions to ascertain: - the source of the money, - the purpose of the MT, - the relationship between the customer and the recipient. ⇒ Consult your supervisor and/or compliance officer to ascertain whether you should proceed with the MT; ⇒ Notify the MTS operator's compliance officer; ⇒ Report the MT (attempt) to the FIU and other LEAs as required.
Illegal gambling[9]	⇒ Customer mentions that MTs are for gambling purposes; ⇒ Customer might mention gambling names (e.g., Poker, Blackjack, or Bingo); ⇒ Customer use phrases like, "this is for my losses," "the odds were against me," "playing cards," or "for the horses"; ⇒ Customer filled out MT forms, putting in information that might have references to gambling.	⇒ In case of suspicions, ask the customer questions to ascertain: - the source of the money, - the purpose of the MT, - the relationship between the customer and the recipient. ⇒ Consult your supervisor and/or compliance officer to ascertain whether you should proceed with the MT; ⇒ Notify the MTS operator's compliance officer;

[9] In some jurisdictions, gambling is illegal or MTS operators may prohibit use of its services for gambling purposes.

Criminal activity	Explanation & Red Flags	Recommendations for FLAs
		⇒ Report the MT (attempt) to the FIU (if applicable).
Fraud (against MT sender)	Customer (sender) might mention as a MT reason the following: ⇒ to help out a close relative/ friend who has got in trouble; ⇒ to get a lottery prize; ⇒ financial support to someone whom the customer has never met in person (e.g. online dating); ⇒ payment for goods / services that are traded on Internet; ⇒ advanced payment for any services to any "service provider' whom the customer has never met in person (employment, taxation, loans, renting, inheritance, etc.).	⇒ In case of suspicions, ask the customer questions to ascertain: - the source of the money, - the purpose of the MT, - the relationship between the customer (sender) and the receiver (*). ⇒ Consult your supervisor and/or compliance officer to ascertain whether you should proceed with the MT; ⇒ Notify the MTS operator's compliance officer; ⇒ Report the MT (attempt) to the FIU (if applicable).
Fraud (by MT receiver)	⇒ Customer (suspect) might be nervous, avoiding eye contact, continuously checking text messages or making calls to inquire for directives; ⇒ Customer admits he/she never met the sender before (but was instructed to tell he/she knew the sender); ⇒ Customer is escorted by other individuals who pretend to be unfamiliar with the customer; ⇒ The information provided by customer does not add up with data recorded in the system (unique MT identifier number, MT amount, originating	⇒ In case of suspicions, ask the customer (suspect) questions to ascertain: - the source of the money, - the purpose of the MT, - the relationship between the customer and the sender (**). ⇒ Make a photo copy of the presented ID, but ask for another; ⇒ When asking questions, watch the customer's behaviour; ⇒ Consult your supervisor and/or compliance

Criminal activity	Explanation & Red Flags	Recommendations for FLAs
	country, sender's name, etc.); ⇒ Customer's ID appears to be altered (personal details, face picture); ⇒ Customer receives multiple MTs (usually during a short period of time, from multiple countries and individuals with whom the customer is not familiar) sent to his/her name which is spelled differently; ⇒ Customer receives MTs sent from the same city/region.	officer to ascertain whether you should proceed with the MT; ⇒ Notify the MTS operator's compliance officer; ⇒ Report the MT (attempt) to the FIU and/or LEAs (if applicable).
Fraud (against MTS provider's FLA)	⇒ Fraudster calls the FLA and with social engineering practices tries to get distance access to the FLA workplace (MTS operating system); ⇒ Fraudster calls the FLA and with social engineering practices tries to force the FLA to initiate a "test transaction" pretending to be a representative of an MTS operator; ⇒ Malware installation and other IT related illegal practices (phishing, authorized access, break password protection etc.).	⇒ Assign a unique code and password that cannot be used by anybody else; ⇒ Update FLA passwords regularly; ⇒ FLA passwords should be complex enough (e.g. KrdKbA5li5 is a reliable password; *1111*, *1234*, *qwert* – are not reliable passwords); ⇒ Design the work place in such a way to prevent unauthorized access and stealing of information; ⇒ Never send test transactions without obtaining the required funds, and if initiated distantly or by a stranger; ⇒ Always check that funds are collected before initiating transaction; ⇒ Never discuss sensitive information with any third party except the authorized representative of MTS operator.

Criminal activity	Explanation & Red Flags	Recommendations for FLAs

(*) Examples of questions the FLA can ask the customer (presumptive victim):

- *Do you know the person you are sending money to?*
- *Does your family member / friend know you are sending him the money?*
- *Did the seller give you an alternative to a MT as the means of payment for the goods or services?*

- The FLA should tell to the customer (presumptive victim) about the suspected fraud.
- The FLA should remember that in case of suspected fraud/ ML/ TF or any other crime, the FLA can always reject the MT, even if the customer insists on its execution.
- At agent's locations, there should be printed leaflets/posters available, as well as lists and the links to online resources[10] about fraud practices.

(**) Examples of questions the FLA might wish to ask the customer who is a suspected fraudster:

- *What is your relationship with the sender?*
- *Where and when did you first meet the sender?*
- *What is the purpose of the transaction?*
- *How often do you use MT services?*
- *Have you been asked to pick up the money by someone else?*

- The FLA should not exhibit aggression even in the case of strong suspicions, and should never tell to the customer (suspected fraudster) about them.
- The FLA may refuse to pay out the MT and under the veil of a technical error, ask the customer to come later if the supervisor and/or compliance officer are unavailable. If they are available, the FLA should act as agreed with the supervisor and/or the compliance officer.

[10] (i) https://www.westernunion.com/us/en/fraudawareness/fraud-awareness-videos; (ii) http://corporate.moneygram.com/compliance/fraud-prevention; (iv) https://international.sigue.com/legal/consumer-fraud-awareness; (v) https://www.youtube.com/watch?v=LBljl8jG218.

ANNEX 7. HIGH-RISK INDUSTRIES FOR THE MTS SECTOR

To protect the company and the customers, MTS operators and their agents should avoid any business relationship that bears uncalculated and/or unmanageable risks. The below examples are such as the following:

Industry	Concern	Recommendation[11]
Unlawful online gambling	Unlawful online gambling can be defined as placing, receiving, or otherwise knowingly transmitting a bet or wager by any means which involves the use, at least in part, of the Internet where such bets or wagers are unlawful under any applicable law in the jurisdiction in which the bet or wager is initiated, received, or otherwise made.	MTS providers should avoid establishing business relationships with any entity involved in unlawful online gambling, or process any payments (MTs) for the purposes of unlawful online gambling.
Shell banks	A shell bank is a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision. The term "physical presence" means meaningful mind and management located within a country. The existence simply of a local Agent or low level staff does not constitute physical presence[12].	MTS providers should not knowingly enter into partnership of any type (agent, subagent), process payments, or allow the use of MTS by shell banks (e.g. B2B services).

[11] This is an aggregated view based on the subjective judgment. The situation can differ from jurisdiction to jurisdiction.
[12] Source: Glossary of the FATF Recommendations

Industry	Concern	Recommendation[11]
Telemarketing	Although telemarketing is usually a legal industry, MTS operators in many jurisdictions are prohibited from servicing these industry players. Since telemarketing outside such jurisdictions can potentially require payments into or out of the jurisdiction which prohibit it, this type of activity should be prohibited globally to minimize the risks.	MTS providers should not knowingly allow for the use of MTS for telemarketing purposes.
Prostitution	Although prostitution may be legal in certain jurisdictions, many MTS operators have found that this business sector can compromise them and cause significant reputational damage.	MTS providers should not knowingly allow for the use of MTs, either by consumers for the purposes related to prostitution or entities involved in the prostitution industry (e.g. P2B/B2P/B2B services).
Marijuana and/or other recreational drugs trade	Although marijuana or other recreational drugs may be legal in certain jurisdictions, many MTS operators have found that doing business with marijuana and/or other recreational drugs traders can expose them to a significant reputational risk.	MTS providers should not knowingly allow the use of MTS either by consumers for the purposes related to marijuana and/or other recreational drug trading, or by entities involved in marijuana and/or other recreational drug trading.
Unlicensed financial service providers	Unlicensed operators put consumers at risk and potentially damage the reputation of the financial services industry.	MTS providers should not knowingly provide MTS or enter into any business partnerships with unlicensed financial service providers (e.g., in some countries these can be Bitcoin industry players).

Industry	Concern	Recommendation[11]
Rough diamond trade	The rough diamond trade is a highly regulated industry. Many jurisdictions have implemented legal acts and have adopted measures stopping the trade in diamonds in conflict zones, and imposing criminal liabilities for breaching rough diamond control regulations [13].	MTS providers should avoid providing MTS to any individual or entity suspected of being involved in the rough diamond trade.
Counterfeit goods	Involvement in the trade of counterfeit goods exposes MTS operators to a significant reputational risk and may result in substantial administrative and/or financial penalties.	MTS providers should not knowingly provide MTS to any individual or entity reasonably suspected of being involved in counterfeit / pirated goods trade.
Other illegal activities	Illegal activities as determined by national and/ or international law.	MTS providers should not knowingly provide MTS to any individual or entity suspected of running illegal businesses or of being involved in illegal activity.

[13] Examples: (1) https://www.globalpolicy.org/the-dark-side-of-natural-resources-st/diamonds-in-conflict/un-documents.html
(2) https://www.treasury.gov/resource-center/sanctions/Documents/diamond.pdf

ANNEX 8. INFORMATION AVAILABLE TO MTS OPERATORs AND THEIR AGENTs

Table 1. Customer and transaction related information available to the agent (Agent, Master Agent, Sub-Agent)

	Type of details	Retail MT	ABMT, Web-based, ATM, SSK, direct to bank MTs	Mobile MT	Pre-paid cards	Business solutions
Customer information (sending agent)	Sender full name	✓	✓	✓	✓(*)	✓(**)
	Payee full name	✓	✓	✓		✓(**)
	Sender DOB	✓	✓	✓	✓	
	Sender COB	✓	✓	✓	✓	
	Sender nationality	✓	✓	✓	✓	
	Sender country of residence	✓	✓	✓	✓	✓(**)
	Sender ID number	✓	✓	✓	✓	✓(**)
	Sender ID type	✓	✓	✓	✓	
	Sender ID date of issuance	✓	✓	✓	✓	
	Sender ID expiry date	✓	✓	✓	✓	
	Sender ID issuing authority	✓	✓	✓	✓	
	Copy of Sender ID	✓	✓	✓	✓	
	Sender address	✓	✓	✓	✓	✓(**)
	Sender phone number	✓	✓	✓	✓	✓(**)
	Sender email address	✓	✓	✓	✓	✓(**)
	Sender occupation	✓	✓	✓	✓	
	Sender tax payer number	✓	✓		✓	
	Sender account number		✓		✓	✓(**)
	Payee account number		✓			✓(**)

	Type of details	Retail MT	ABMT, Web-based, ATM, SSK, direct to bank MTs	Mobile MT	Pre-paid cards	Business solutions
Customer information (receiving agent)	Sender full name	✓	✓	✓		✓(**)
	Payee full name	✓	✓	✓		✓(**)
	Sender DOB	✓(***)	✓	✓		
	Sender COB	✓(***)	✓	✓		
	Sender ID number	✓(***)	✓	✓		
	Sender address	✓(***)	✓	✓		
	Payee DOB	✓	✓	✓		
	Payee COB	✓	✓	✓		
	Payee nationality	✓	✓	✓		
	Payee country of residence	✓	✓	✓		✓(**)
	Payee ID number	✓	✓	✓		✓(**)
	Payee ID type	✓	✓	✓		
	Payee ID date of issuance	✓	✓	✓		
	Payee ID expiry date	✓	✓	✓		
	Payee ID issuing authority	✓	✓	✓		
	Copy of Payee ID	✓	✓	✓		
	Payee address	✓	✓	✓		✓(**)
	Payee phone number	✓	✓	✓		✓(**)
	Payee email address	✓	✓	✓		✓(**)
	Payee occupation	✓	✓	✓		
	Payee tax payer number	✓	✓	✓		
	Sender account number		✓			✓(**)

	Type of details	Retail MT	ABMT, Web-based, ATM, SSK, direct to bank MTs	Mobile MT	Pre-paid cards	Business solutions
	Payee account number		✓			✓(**)
Transaction related information	Transaction identifier (#)	✓	✓	✓	✓	✓
	Internal customer identifier	✓	✓	✓	✓	✓
	Test question/answer	✓	✓			
	Send and pay country	✓	✓	✓	✓	✓
	Send amount and currency	✓	✓	✓	✓	✓
	Pay amount and currency	✓	✓	✓	✓	✓
	Transaction fee amount (****)	✓	✓	✓	✓	✓
	Date and time of send/pay (****)	✓	✓	✓	✓	✓
	Type of product/service	✓	✓	✓	✓	✓
	Customer PC/device IP/ID		✓	✓		
	Agent code/name	✓	✓	✓	✓	✓
	Location code/name/address (****)	✓			✓	✓
	FLA name and identifier (****)	✓			✓	✓
	Sender bank name		✓		✓	✓
	Payee bank name		✓		✓	✓
	Purpose of transaction	✓	✓	✓	✓	✓
	Availability of supporting documentation for purpose of transaction	✓	✓	✓	✓	✓

	Type of details	Retail MT	ABMT, Web-based, ATM, SSK, direct to bank MTs	Mobile MT	Pre-paid cards	Business solutions
	Source of funds	✓	✓	✓	✓	✓
	Availability of supporting documentation for source of funds	✓	✓	✓	✓	✓
	Sender/Payee PEP status	✓	✓	✓	✓	
	Sender/Payee sanctions screening results	✓	✓	✓	✓	✓
	Copy of to send/pay form (****)	✓	✓	✓	✓	✓

(*) In the context of pre-paid card MTs, the "Sender" refers to the bankcard owner.

(**) In terms of business-to-business transactions, the Sender/Payee details should be understood as business entity details (e.g. entity name, entity account number, entity address, entity registration number, etc.).

(***) Set of Sender details may be extended depending on the legislative requirements in the destination country.

(****) Sending and receiving agents have access only to their data; MTS operator has access to all data.

MTS operators have direct access to ALL information listed in the Table 1. In addition, MTS operators retain information about all their agents as specified in the Table 2.

Table 2. Agent (Agent, Master Agent, Sub-Agent) related information available to MTS operator.

Type of details	Retail MTs	ABMT, Web-based, ATM, SSK, direct-to-bank MTs	Mobile money transfers	Pre-paid cards	Business solutions
Agent name and details (*)	✓	✓	✓	✓	✓
Location code/ name/ address	✓			✓	✓
FLA name and identifier	✓			✓	✓
Type of product/ service	✓	✓	✓	✓	✓
Transaction lifecycle records (**)	✓	✓	✓	✓	✓

(*) Set of Agent details depends on local legislative requirements and MTS operator's KYA provisions, and goes far beyond the basic details such as name and address, and usually includes a wide range of entity-related information and documents such as type of business, copies of licenses, shareholder and top management structure, personal details of top managers and controlling persons, internal policies and procedures, etc.

(**) History of all modifications to any transaction made by an FLAs at any time, for example, "send", "pay", "view", "cancel", "refund", etc.

The MTS operator should retain and as such be able to share the compliance monitoring records on the customers (monitoring and analysis of customers' activity, information and documents collected with ECDD) and the agents (analysis of agents' activity – at a location level, an FLA level, country and global level), information and documents collected within agents' EDD, on-site and off-site checks and inspections).

Summary notes for the Tables 1 and 2:

1. Set of collected customer details differs from country to country depending on local legislative requirements, product/service used, the MTS operator's and the agents' internal policies and procedures. Thus, the list provided in the Table 1 may be non-exhaustive or not completely accurate.

2. Sub-Agent and Agent have access to the information about the customers and the transactions that took place at their points of sale only.

3. Master Agent has access to the information about the customers and the transactions that took place with its locations network, as well as access to electronic (only) customer and transaction related information of its agents (copies of supporting documentation may be provided upon request).

4. MTS operator has direct access to all customer and transaction related information including all type of agents. However, customer and transaction related documentation is not available unless the MTS operator has performed the MTS directly; but this may be provided by the agents upon MTS operator's request.

5. Collecting and verification of the customers' IDs is possible in case of retail MTs (at a point of sale) and usually is not required (depends on the local legislation). In Turkey, for example, retaining customer's ID is mandatory. In Ukraine, it is not required; however, many agents retain both hard and soft copies of the customers' IDs. In case of remote transactions (web-based, through ATM, SSK, or direct-to-bank MTs), ID copies can also be collected in scanned form, but their validity will require additional verification actions, such as the requirement for the customer to visit the agent's point of sale for the initial registration for ABMT services, or through verification of ID copies via domestic governmental ID database, if applicable.

6. Upon the successful completion of a retail MT (at a point of sale), either inbound or outbound MTs, agents collect MT paper forms completed and signed by the customers.

ANNEX 9. THE FATF STANDARDS ON INFORMATION EXCHANGE APPLICABLE TO THE MTS SECTOR[14]

#	RELEVANT EXCERPTS	PARTIES EXCHANGING	SOURCE
	in relation to money transfers		
1.	Countries should ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain.	Private ⇔ Private	R.16
2.	Countries may adopt a *de minimis* threshold for cross-border wire transfers (no higher than USD/EUR 1,000), below which the following requirements should apply: (a) Countries should ensure that financial institutions include with such transfers: (i) the name of the originator; (ii) the name of the beneficiary; and (iii) an account number for each, or a unique transaction reference number. Such information need not be verified for accuracy, unless there is a suspicion of money laundering or terrorist financing, in which case, the financial institution should verify the information pertaining to its customer. (b) Countries may, nevertheless, require that incoming cross-border wire transfers below the threshold contain required and accurate originator information.	Private ⇔ Private	INR.16, §5
3.	Information accompanying all qualifying wire transfers should always contain: (a) the name of the originator; (b) the originator account number where such an account is used to process the transaction; (c) the originator's address, or national identity number, or customer identification number[15], or date and place of birth; (d) the name of the beneficiary; and (e) the beneficiary account number where such an account is used to process the transaction.	Private ⇔ Private	INR.16, §6

4.	In the absence of an account, a unique transaction reference number should be included which permits traceability of the transaction.	Private ⇔ Private	INR.16, §7
5.	Information accompanying domestic wire transfers should also include originator information as indicated for cross-border wire transfers, unless this information can be made available to the beneficiary financial institution and appropriate authorities by other means. In this latter case, the ordering financial institution need only include the account number or a unique transaction reference number, provided that this number or identifier will permit the transaction to be traced back to the originator or the beneficiary.	Private ⇔ Private	INR.16, §9
6.	The information should be made available by the ordering financial institution within three business days of receiving the request either from the beneficiary financial institution or from appropriate competent authorities. Law enforcement authorities should be able to compel immediate production of such information.	Private ⇔ Private Private ⇔ Public	INR.16, §10
7.	The ordering financial institution should ensure that qualifying wire transfers contain required and accurate originator information, and required beneficiary information.	Private ⇔ Private	INR.16, §11
8.	The ordering financial institution should ensure that cross-border wire transfers below any applicable threshold contain the name of the originator and the name of the beneficiary and an account number for each, or a unique transaction reference number.	Private ⇔ Private	INR.16, §12
9.	The ordering financial institution should maintain all originator and beneficiary information collected, in accordance with Recommendation 11.	Private ⇔ Private	INR.16, §13
10.	The ordering financial institution should not be allowed to execute the wire transfer if it does not comply with the requirements specified above.	Private ⇔ Private	INR.16, §14

[14] Items 23-28 apply to all types of customer and transaction related information.

[15] The customer identification number refers to a number which uniquely identifies the originator to the originating financial institution and is a different number from the unique transaction reference number. The customer identification number must refer to a record held by the originating financial institution which contains at least one of the following: the customer address, a national identity number, or a date and place of birth.

11.	For cross-border wire transfers, financial institutions processing an intermediary element of such chains of wire transfers should ensure that all originator and beneficiary information that accompanies a wire transfer is retained with it.	Private ⇔ Private	INR.16, §15
12.	Where technical limitations prevent the required originator or beneficiary information accompanying a cross-border wire transfer from remaining with a related domestic wire transfer, a record should be kept, for at least five years, by the receiving intermediary financial institution of all the information received from the ordering financial institution or another intermediary financial institution.	Private ⇔ Private	INR.16, §16
13.	A beneficiary financial institution should take reasonable measures to identify cross-border wire transfers that lack required originator or required beneficiary information. Such measures may include post-event monitoring or real-time monitoring where feasible.	Private ⇔ Private	INR.16, §19
14.	For qualifying wire transfers, a beneficiary financial institution should verify the identity of the beneficiary, if the identity has not been previously verified, and maintain this information in accordance with Recommendation 11.	Private ⇔ Private	INR.16, §20
15.	A beneficiary financial institution should have effective risk-based policies and procedures for determining: (i) when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and (ii) the appropriate follow-up action.	Private ⇔ Private	INR.16, §21
16.	In the case of a MVTS provider that controls both the ordering and the beneficiary side of a wire transfer, the MVTS provider: (a) should take into account all the information from both the ordering and beneficiary sides in order to determine whether an STR has to be filed; and (b) should file an STR in any country affected by the suspicious wire transfer, and make relevant transaction information available to the Financial Intelligence Unit.	Private ⇔ Public	INR.16, §22

17.	If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (FIU).	Private ⇔ Public	R.20
18.	All suspicious transactions, including attempted transactions, should be reported regardless of the amount of the transaction.	Private ⇔ Public	INR.20, §3
19.	The reporting requirement should be a direct mandatory obligation, and any indirect or implicit obligation to report suspicious transactions, whether by reason of possible prosecution for a money laundering or terrorist financing offence or otherwise (so called "indirect reporting"), is not acceptable.	Private ⇔ Public	INR.20, §4
20.	The FIU serves as the central agency for the receipt of disclosures filed by reporting entities. At a minimum, this information should include suspicious transaction reports, as required by Recommendation 20 and 23, and it should include other information as required by national legislation (such as cash transaction reports, wire transfers reports and other threshold-based declarations/disclosures).	Private ⇔ Public	INR.29, §2
21.	In addition to the information that entities report to the FIU (under the receipt function), the FIU should be able to obtain and use additional information from reporting entities as needed to perform its analysis properly. The information that the FIU should be permitted to obtain could include information that reporting entities are required to maintain pursuant to the relevant FATF Recommendations (Recommendations 10, 11 and 22).	Private ⇔ Public	INR.29, §5
22.	When conducting investigations of money laundering, associated predicate offences and terrorist financing, competent authorities should be able to obtain access to all necessary documents and information for use in those investigations, and in prosecutions and related actions. This should include powers to use compulsory measures for the production of records held by financial institutions, DNFBPs and other natural or legal persons [...]	Private ⇔ Public	R.31
23.	The FIU [...] should have access on a timely basis to the financial, administrative and law enforcement information that it requires to undertake its functions properly.	Public ⇔ Public (nationally)	R.29,

	The FIU should be able to disseminate, spontaneously and upon request, information and the results of its analysis to relevant competent authorities [...] In order to conduct proper analysis, the FIU should have access to the widest possible range of financial, administrative and law enforcement information. This should include [...] relevant information collected and/or maintained by, or on behalf of, other authorities [...] The FIU should also be able to make arrangements or engage independently with other domestic competent authorities or foreign counterparts on the exchange of information.		INR.29, §§4,6,11
24.	Countries should ensure that their competent authorities can rapidly, constructively and effectively provide the widest range of international cooperation in relation to money laundering, associated predicate offences and terrorist financing. Countries should do so both spontaneously and upon request, and there should be a lawful basis for providing cooperation. Countries should authorise their competent authorities to use the most efficient means to cooperate. Should a competent authority need bilateral or multilateral agreements or arrangements, such as a Memorandum of Understanding (MOU), these should be negotiated and signed in a timely way with the widest range of foreign counterparts. Competent authorities should use clear channels or mechanisms for the effective transmission and execution of requests for information or other types of assistance. Competent authorities should have clear and efficient processes for the prioritisation and timely execution of requests, and for safeguarding the information received. When making requests for cooperation, competent authorities should make their best efforts to provide complete factual and, as appropriate, legal information, including indicating any need for urgency, to enable a timely and efficient execution of the request, as well as the foreseen use of the information requested. Upon request, requesting competent authorities should provide feedback to the requested competent authority on the use and usefulness of the information obtained. Countries should not prohibit or place unreasonable or unduly restrictive conditions on the provision of exchange of information or assistance. In particular competent authorities should not refuse a request for	Public ⇔ Public (internationally, general provisions)	R.40,

	assistance on the grounds that: (a) the request is also considered to involve fiscal matters; and/or (b) laws require financial institutions or DNFBPs (except where the relevant information that is sought is held in circumstances where legal privilege or legal professional secrecy applies) to maintain secrecy or confidentiality; and/or (c) there is an inquiry, investigation or proceeding underway in the requested country, unless the assistance would impede that inquiry, investigation or proceeding; and/or (d) the nature or status (civil, administrative, law enforcement, etc.) of the requesting counterpart authority is different from that of its foreign counterpart. […] Exchange of information should take place in a secure way, and through reliable channels or mechanisms […] Competent authorities should be able to conduct inquiries on behalf of a foreign counterpart, and exchange with their foreign counterparts all information that would be obtainable by them if such inquiries were being carried out domestically. The general principles above should apply to all forms of exchange of information between counterparts or non-counterparts, subject to the paragraphs set out below.		INR.40, §§1,2,4,5,6

25.	FIUs should exchange information with foreign FIUs, regardless of their respective status; be it of an administrative, law enforcement, judicial or other nature. To this end, FIUs should have an adequate legal basis for providing cooperation on money laundering, associated predicate offences and terrorist financing. When making a request for cooperation, FIUs should make their best efforts to provide complete factual, and, as appropriate, legal information, including the description of the case being analysed and the potential link to the requested country. Upon request and whenever possible, FIUs should provide feedback to their foreign counterparts on the use of the information provided, as well as on the outcome of the analysis conducted, based on the information provided. FIUs should have the power to exchange: (a) all information required to be accessible or obtainable directly or indirectly by the FIU under the FATF Recommendations, in particular under Recommendation 29; and (b) any other information which they have the power to obtain or access, directly or indirectly, at the domestic level, subject to the principle of reciprocity.	Public ⇔ Public (internationally, FIU-FIU)	INR.40, §§7,8,9

26.	Financial supervisors should cooperate with their foreign counterparts, regardless of their respective nature or status. Efficient cooperation between financial supervisors aims at facilitating effective AML/CFT supervision of financial institutions. To this end, financial supervisors should have an adequate legal basis for providing cooperation, consistent with the applicable international standards for supervision, in particular with respect to the exchange of supervisory information related to or relevant for AML/CFT purposes. Financial supervisors should be able to exchange with foreign counterparts information domestically available to them, including information held by financial institutions, and in a manner proportionate to their respective needs. Financial supervisors should be able to exchange the following types of information when relevant for AML/CFT purposes, in particular with other relevant supervisors that have a shared responsibility for financial institutions operating in the same group: (a) Regulatory information, such as information on the domestic regulatory system, and general information on the financial sectors. (b) Prudential information, in particular for Core Principle Supervisors, such as information on the financial institution's business activities, beneficial ownership, management, and fit and properness. (c) AML/CFT information, such as internal AML/CFT procedures and policies of financial institutions, customer due diligence information, customer files, samples of accounts and transaction information. Financial supervisors should be able to conduct inquiries on behalf of foreign counterparts, and, as appropriate, to authorise or facilitate the ability of foreign counterparts to conduct inquiries themselves in the country, in order to facilitate effective group supervision.	Public ⇔ Public (internationally, between financial supervisors)	INR.40, §§10,11,12

27.	Law enforcement authorities should be able to exchange domestically available information with foreign counterparts for intelligence or investigative purposes relating to money laundering, associated predicate offences or terrorist financing, including the identification and tracing of the proceeds and instrumentalities of crime. Law enforcement authorities should also be able to use their powers, including any investigative techniques available in accordance with their domestic law, to conduct inquiries and obtain information on behalf of foreign counterparts. The regimes or practices in place governing such law enforcement cooperation, such as the agreements between Interpol, Europol or Eurojust and individual countries, should govern any restrictions on use imposed by the requested law enforcement authority. Law enforcement authorities should be able to form joint investigative teams to conduct cooperative investigations, and, when necessary, countries should establish bilateral or multilateral arrangements to enable such joint investigations. Countries are encouraged to join and support existing AML/CFT law enforcement networks, and develop bi-lateral contacts with foreign law enforcement agencies, including placing liaison officers abroad, in order to facilitate timely and effective cooperation.	Public ⇔ Public (internationally, LE-LE)	INR.40, §§14,15,16
28.	Countries should permit their competent authorities to exchange information indirectly with non-counterparts, applying the relevant principles above. Indirect exchange of information refers to the requested information passing from the requested authority through one or more domestic or foreign authorities before being received by the requesting authority. Such an exchange of information and its use may be subject to the authorisation of one or more competent authorities of the requested country. The competent authority that requests the information should always make it clear for what purpose and on whose behalf the request is made. Countries are also encouraged to permit a prompt and constructive exchange of information directly with non-counterparts.	Public ⇔ Public (internationally, between non-counterparts)	INR.40, §§17,18

in relation to ML/TF risks			
29.	Countries should take appropriate steps to identify and assess the money laundering and terrorist financing risks for the country, on an ongoing basis and in order to: [...] (iii) make information available for AML/CFT risk assessments conducted by financial institutions [...]. Countries should keep the assessments up-to-date, and should have mechanisms to provide appropriate information on the results to all relevant [...] self-regulatory bodies (SRBs), financial institutions and DNFBPs.	Public ⇔ Private	INR.1, §3
30.	Where countries identify higher risks, they should ensure that their AML/CFT regime addresses these higher risks and [...] either prescribe that financial institutions and DNFBPs take enhanced measures to manage and mitigate the risks, or ensure that this information is incorporated into risk assessments carried out by financial institutions and DNFBPs, in order to manage and mitigate risks appropriately.	Public ⇔ Private	INR.1, §4
31.	Financial institutions and DNFBPs should be required to take appropriate steps to identify and assess their money laundering and terrorist financing risks [...] and have appropriate mechanisms to provide risk assessment information to competent authorities and SRBs [...].	Private ⇔ Public	INR.1, §8
32.	There should be effective measures in place to ensure that financial institutions are advised of concerns about weaknesses in the AML/CFT systems of other [high risk] countries.	Public ⇔ Private	INR.19, §2(b)
33.	[...] supervisors and SRBs should, as and when required in accordance with the Interpretive Notes to Recommendations 26 and 28, review the money laundering and terrorist financing risk profiles and risk assessments prepared by financial institutions and DNFBPs, and take the result of this review into consideration.	Public ⇔ Private	INR.1, §7
34.	[...] supervisors: [...] (b) should have on-site and off-site access to all relevant information on the specific domestic and international risks associated with customers, products and services of the supervised institutions, including the quality of the compliance function of the financial institution or group [...].	Private ⇔ Public	INR.26, §2
35.	Supervisors should [...] be authorised to compel production of any information from financial institutions that is relevant to monitoring such compliance.	Private ⇔ Public	R.27

36.	Countries should keep the assessments up-to-date, and should have mechanisms to provide appropriate information on the results to all relevant competent authorities [...]	Public ⇔ Public	INR.1, §3
	in relation to customers		
37.	If, during the establishment or course of the customer relationship, or when conducting occasional transactions, a financial institution suspects that transactions relate to money laundering or terrorist financing, then the institution should: [...] (b) make a suspicious transaction report (STR) to the financial intelligence unit (FIU), in accordance with Recommendation 20.	Private ⇔ Public	INR.10, §1(b)
38.	If the institution reasonably believes that performing the CDD process will tip-off the customer or potential customer, it may choose not to pursue that process, and should file an STR [...].	Private ⇔ Public	INR.10, §3
39.	Countries may permit financial institutions to rely on third parties to perform elements (a)-(c) of the CDD measures set out in Recommendation 10 or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for CDD measures remains with the financial institution relying on the third party. The criteria that should be met are as follows: (a) A financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a)-(c) of the CDD measures set out in Recommendation 10. (b) Financial institutions should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay. (c) The financial institution should satisfy itself that the third party is regulated, supervised or monitored for, and has measures in place for compliance with, CDD and record-keeping requirements in line with Recommendations 10 and 11. (d) When determining in which countries the third party that meets the conditions can be based, countries should have regard to information available on the level of country risk.	Private ⇔ Private	R.17

	When a financial institution relies on a third party that is part of the same financial group, and (i) that group applies CDD and record-keeping requirements, in line with Recommendations 10, 11 and 12, and programmes against money laundering and terrorist financing, in accordance with Recommendation 18; and (ii) where the effective implementation of those CDD and record-keeping requirements and AML/CFT programmes is supervised at a group level by a competent authority, then relevant competent authorities may consider that the financial institution applies measures under (b) and (c) above through its group programme, and may decide that (d) is not a necessary precondition to reliance when higher country risk is adequately mitigated by the group AML/CFT policies.		
in relation to money transfers related records			
40.	Financial institutions should be required to maintain, for at least five years, all necessary records on transactions, both domestic and international, to enable them to comply swiftly with information requests from the competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide, if necessary, evidence for prosecution of criminal activity [...] The CDD information and the transaction records should be available to domestic competent authorities upon appropriate authority.	Private ⇔ Public	R.11
in relation to agents			
41.	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 [...]	Private ⇔ Public	R.14
in relation to guidance and feedback			
42.	The competent authorities, supervisors and SRBs should establish guidelines, and provide feedback, which will assist financial institutions and designated nonfinancial businesses and professions in applying national measures to combat money laundering and terrorist financing, and, in particular, in detecting and reporting suspicious transactions.	Public ⇔ Private	R.34