



Global Partner Compliance Policy

Version 1
2016



Global Partner Compliance Policy

Purpose of Policy. MoneyGram Agents¹ and other non-agent distribution channels² are important partners in offering MoneyGram money transfer and other services and products to our valued consumers. Because MoneyGram and its partners are required to comply with various laws and governmental regulations worldwide, MoneyGram has issued this *Global Partner Compliance Policy* (“Policy”).

Agents and their employees are part of the first line of defense in protecting consumers and preventing criminal abuse and exploitation of MoneyGram products and services. The Policy outlines the responsibilities of Agents globally to comply with applicable laws and regulations, with MoneyGram’s policies and procedures, and the required actions for effective implementation of strict anti-money laundering and anti-fraud standards.

This Policy also reinforces MoneyGram’s commitment to protecting its consumers and to preventing the use of its products and services by anyone for fraudulent purposes, money laundering, terrorist financing, or other illegal activities. MoneyGram requires the same commitment from its Agents and their owners, shareholders, governing authorities, management, and employees. Agents are responsible for implementing this Policy. To carry out this Policy, MoneyGram has incorporated herein the key requirements that govern the relationship between MoneyGram and its Agents.

MoneyGram continues to update its Anti-Money Laundering and Anti-Fraud Compliance Programs (“Programs”) to review and respond to issues related to the implementation of this Policy. MoneyGram encourages its Agents to contact the MoneyGram Regional Compliance Officer or other compliance contact assigned to the Agent regarding questions about this Policy.

1 OPERATE IN A LEGAL AND ETHICAL MANNER

The overarching duty of Agents and their employees is to operate in a legal and ethical manner. This includes not only an Agent’s full compliance with applicable laws and regulations, but also an expectation that MoneyGram’s partners conduct themselves with honesty and integrity as they offer MoneyGram’s products and services to consumers. The reputation of Agents and their employees directly reflects on MoneyGram’s own reputation. Therefore, MoneyGram sets forth below the policy statements that govern the conduct of Agents and their employees.

¹ The definition of Agent includes any party entering into a contractual relationship with MoneyGram or its subsidiaries and affiliates for the purposes of providing MoneyGram’s products and services to consumers. This definition also includes all Subagents of an Agent.

² MoneyGram distributes some products and services through arrangements that are not traditional principal/Agent relationships. MoneyGram does conduct oversight of these distribution channels. Given the differences in the products and services offered or the differences in the regulatory requirements applicable to these distribution channels, the non-agent distribution channel’s obligations may vary and will be spelled out in detail in their contract with MoneyGram.



- 1.1 Agents and their employees shall operate in compliance with applicable laws and regulations in all countries and jurisdictions where they do business.
 - Agents shall obtain, maintain, and post any required registrations or licenses as required by national, state/provincial, or local laws or regulations.
 - Agents and their employees shall not participate in, or knowingly facilitate fraud, money laundering, terrorist financing, or other illegal activities.
 - Agents shall monitor potentially suspicious locations and employee activity, including when an employee or location is involved in an excessive number of unresolved transaction exceptions or potentially suspicious transactions or exhibits unusual behavior warranting investigation. If a location or employee is suspected of complicity or participation in illegal activity, the Agent shall take action as outlined in this Policy.
- 1.2 Agents and their employees shall conduct themselves with honesty, integrity, and unquestionable ethical standards, including, but not limited to the following:
 - Agents and their employees shall deal honestly and fairly with those with whom they interact in the provision of MoneyGram's products and services. Agents and their employees shall not take actions that could damage MoneyGram's reputation with its consumers, suppliers, service providers, competitors, and government officials.
 - Agents and their employees shall not complete a transaction if it is suspected that the transaction is related to any unlawful activity. MoneyGram products and services should only be used for legal purposes.
 - Agents and their employees shall not violate this Policy, including providing false or misleading information to MoneyGram, consumers, law enforcement, or regulators.
- 1.3 Agents shall act to stop violations of this section and report concerns to the appropriate person.
 - If an Agent or their employee becomes aware of any information that leads them to believe that any Agent or employee has failed to comply with this section of the Policy, they shall report that information to the MoneyGram Regional Compliance Officer assigned to the Agent, MoneyGram's Chief Compliance Officer, or MoneyGram's Compliance Hotline (see Important Contact Information).



- If an Agent or their employee becomes aware of any information that leads them to believe that MoneyGram or any MoneyGram employee has engaged in unethical, improper, or illegal conduct or failed to comply with any applicable governmental law, rule or regulation, they shall report that information to the MoneyGram Regional Compliance Officer assigned to the Agent, MoneyGram's Chief Compliance Officer, or MoneyGram's Compliance Hotline.
- Agents and their employees may report a suspected violation on an anonymous basis by using MoneyGram's Compliance Hotline. MoneyGram will make every reasonable effort to ensure the confidentiality of those furnishing information, unless MoneyGram is required by law or regulation(s) to disclose the information.
- MoneyGram does not tolerate retaliation under any circumstances including, but not limited to, retaliation against anyone who has made an allegation, reported a violation, or provided information as part of an investigation. If an Agent or their employee believes they have been subjected to retaliation or they know about an incident of retaliation, they shall immediately report the alleged retaliation to the MoneyGram Regional Compliance Officer assigned to the Agent, MoneyGram's Chief Compliance Officer, or MoneyGram's Compliance Hotline.

1.4 Agents and their employees shall provide accurate and complete information to MoneyGram, law enforcement, or regulatory authorities in accordance with applicable laws and regulations. This includes, but is not limited to the following situations:

- when entering information into MoneyGram's systems, providing the information in-person to MoneyGram's employees or during Agent Program Reviews;
- where MoneyGram has requested information on transactions or the Agent's anti-money laundering and anti-fraud programs;
- during the application process, contract renewal, refreshed Agent file or due diligence reviews, compliance reviews, or where reasonably requested by MoneyGram;
- when there are any material change(s) in the ownership and/or senior management of the Agent; and
- where lawfully requested by law enforcement or civil regulators.



2 PROHIBITION AGAINST BRIBERY AND CORRUPTION

Various laws around the world prohibit the making of improper payments or providing improper gifts or hospitality to secure business or to gain an unfair business advantage. As a company headquartered in the United States, MoneyGram is subject to the Foreign Corrupt Practices Act (“FCPA”) and other federal and state commercial bribery laws, as well as applicable anti-corruption and commercial bribery laws in the various countries in which MoneyGram operates, including the United Kingdom’s Bribery Act (“UKBA”). MoneyGram expects that its Agents and their employees conduct business affairs in a manner beyond reproach, including compliance with applicable anti-corruption laws, especially the Foreign Corrupt Practices Act and the United Kingdom’s Bribery Act.

2.1 Agents and their employees shall not engage in bribery or corruption in order to secure an undue advantage in connection with MoneyGram’s business, including the offering of MoneyGram’s products and services. This prohibition applies to any transactions involving either Government Officials or Commercial Parties.

The term “Government Official” includes:

- Officers and employees of any government department, agency, commission, bureau, or authority, at any level of government (national, state or provincial, regional, or local), whether they are elected, career employees, or political appointees;
- Legislators and judges;
- Any persons acting in an official capacity on behalf of a public authority;
- Officers and employees of entities that are owned or controlled by a public authority;
- Candidates for political office;
- Officers and employees of a political party, as well as the political party as an institution/entity;
- Officers and employees of any Public International Organization; and
- Anyone else treated as a government official under local laws of the locations where MoneyGram operates.
- A “Commercial Party” is any company, organization, or commercial entity whose personnel do not qualify as “Government Officials,” including any employee, agent, trustee, or fiduciary of such party.

2.2 Agents shall maintain adequate compliance controls to prevent, discourage, and detect potential violations of this section in the Policy and applicable anti-bribery and anti-corruption laws.



3 MAINTAIN AN EFFECTIVE ANTI-MONEY LAUNDERING AND ANTI-FRAUD PROGRAMS

Agents play an important role in preventing MoneyGram's products and systems, and the financial system at large, from being used for criminal activity. To that end, MoneyGram requires its Agents to follow this Policy and implement anti-money laundering and anti-fraud programs. However, Agents are not without support as they implement this Policy. MoneyGram provides support to its Agents in a variety of ways, including offering training and educational materials to Agents, such as materials to help Agents document and carry out their anti-money laundering and anti-fraud programs. In addition, MoneyGram assists in ensuring the effectiveness of the Agent's compliance program through evaluation conducted at on-boarding and on an ongoing basis. MoneyGram seeks an open channel of communication with Agents as they fulfill the obligations set forth below.

3.1 MoneyGram Agents shall implement and adhere to written, effective, risk-based policies and programs sufficient to assist in the prevention of consumer fraud and to meet applicable anti-money laundering, compliance, and/or other regulatory requirements.

- Agents shall conduct their operations using a risk-based approach, as demonstrated by the adoption and implementation of the transaction monitoring and reporting systems described below, and should have an understanding of the risk of money laundering and fraud presented by the geographic location(s) of the Agent, the consumers served by the Agent, and products offered by the Agent.
- Agents shall adopt and implement anti-money laundering and anti-fraud programs, based on the risk of the Agent's business, that meet, at a minimum, the following requirements:
 - Address the designation of a compliance officer, employee training, transaction monitoring and reporting, collecting and maintaining consumer information and, if required, independent review of the Agent's anti-money laundering and anti-fraud programs. These requirements are outlined in more detail below;
 - Receive approval from the Agent's ownership and management, including a commitment to support and adhere to this Policy and the Agent's anti-money laundering and anti-fraud programs;
 - Implement effective programs to monitor transactions and attempted transactions performed at their locations and, report suspicious activity to the relevant authorities as required by applicable laws, and/or escalate the



information to MoneyGram. Some examples of situations which must be escalated to MoneyGram include the following:

- Agent believing that the suspicious activity is likely occurring beyond or outside of their network and may involve additional MoneyGram Agent locations outside of their network (if applicable);
 - Agent being concerned about a cross-border transfer and believing that law enforcement outside of their country should be made aware;
 - Agent identifying what they believe is an emerging suspicious or unusual pattern or trend; or
 - Agent being concerned that the transaction may involve terrorist financing. If this is the case, the Agent should contact MoneyGram and law enforcement immediately.
 - If the Agent is in a country that requires that the reporting of suspicious activity must come directly from MoneyGram, the results of the monitoring, as well as any related information, must be provided by the Agent to MoneyGram within a reasonable time or as required by any applicable law or regulation.
-
- Monitor transactions for potentially suspicious or unusual activities, such as the potential structuring of transactions to evade legal and/or regulatory reporting requirements, the evasion of identification requirements, the practice of sharing identification documents, and any other unusual behaviors such as one person sending to many individuals in many different countries;
 - Document the results of anti-money laundering and anti-fraud monitoring, including the filing of any suspicious activity reports with the applicable regulator and/or escalating potentially suspicious activity to MoneyGram;
 - Provide written policies and procedures for employees to follow to detect and prevent fraud-induced, structured or otherwise illicit money transfers or transactions;
 - Provide written policies and procedures for employees to follow to report potentially suspicious activity, or large currency transactions, and fulfill any other regulatory reporting obligations in the jurisdiction in which the Agent operates. Such policies and procedures should address obligations regarding “no tipping off” a consumer when suspicious activity has been reported; and
 - Provide guidance to employees on how to escalate potentially suspicious activity to MoneyGram when necessary.



- Agents within the United States as well as Agents outside the United States with ten or more locations shall complete risk-based, independent reviews to evaluate the effectiveness of the Agent’s anti-money laundering and anti-fraud programs (“Independent Reviews”). These Independent Reviews shall be conducted periodically or as often as required by applicable laws, regulations, or MoneyGram. Independent Reviews shall be documented in writing and the Agent shall document the actions it has taken in response to any deficiencies identified by the Independent Reviews. Independent Reviews shall consider the adequacy of the Agent’s:
 - written anti-money laundering and anti-fraud programs;
 - authority and expertise of the Agent’s compliance officer;
 - employee training;
 - transaction monitoring and reporting, including the filing of suspicious activity reports and/or escalating suspicious activity to MoneyGram, when necessary; and
 - any other deficiencies related to the implementation of and adherence to this Policy.
- Agents shall designate a compliance officer responsible for implementation and adherence to the Agent’s anti-money laundering and anti-fraud programs. This compliance officer must, at a minimum, meet the following requirements:
 - committed to support and adhere to this Policy and the Agent’s anti-money laundering and anti-fraud programs;
 - capable to implement and maintain the Agent’s anti-money laundering and anti-fraud programs;
 - vested with the appropriate authority to implement the Agent’s anti-money laundering and anti-fraud programs throughout the network, if applicable;
 - supported by the Agent’s ownership and management, and titled as an officer or manager with direct lines of communication to ownership or management;
 - authorized to ensure risk-based Independent Reviews of the Agent’s anti-money laundering and anti-fraud programs, if applicable; and



- knowledgeable about the Agent’s day-to-day business, including the offering of MoneyGram’s products and services.
- Agents shall ensure there is sufficient staffing and resources to adequately implement this Policy and the policies and programs the Agent has adopted.
- Any delegation or distribution of duties under this Policy shall be clearly set forth in writing by the Agent and agreed to by the Subagents (applicable to only certain Agent relationships outside the United States). Regardless of any delegation or distribution of duties, Agents shall ensure that Subagents operating under the Agent adhere to the requirements of this Policy.

4 AGENT EMPLOYEE TRAINING

As stated above, Agents and their employees are the first line of defense in protecting consumers and preventing criminal abuse and exploitation of MoneyGram products and services. Agent and employees must be provided the training and tools necessary to prevent errors or abuse from occurring in the use of MoneyGram’s products and services. Moreover, as part of employee training, Agents should communicate to their employees that the Agent’s management supports full compliance with applicable laws and regulations. MoneyGram requires that Agents only permit properly trained employees to provide MoneyGram’s products and services to consumers.

- 4.1 Agents shall ensure employees are sufficiently trained to process transactions using MoneyGram’s systems and will adhere to this Policy and the Agent’s anti-money laundering and anti-fraud programs. MoneyGram is continuously improving its policies and programs and may update Agent responsibilities at any time based on changes in laws, regulations, industry best practices, or risk. Agents are responsible for communicating those changes to their employees and any Subagents (applicable to only certain Agent relationships outside the United States) and ensuring their implementation.
- 4.2 Agents shall train all employees who interact with consumers using MoneyGram’s products and services on anti-money laundering and anti-fraud measures using either the training provided by MoneyGram or equivalent training. This training shall occur at least every two years or more frequently as required by local laws or regulations or by MoneyGram. This training shall include the following:
 - adherence to all requirements set forth in this Policy;
 - identification of consumer scams and prevention of fraud-induced transfers;
 - verification of consumer identification;



- compliance with all relevant transaction processing requirements, including correct data collection and entry procedures;
- identification and reporting suspicious activity and structured transactions; and
- satisfying record retention requirements.

4.3 Agents are responsible for ensuring employees understand their responsibilities and provide refreshed training to employees as necessary. In addition, Agents shall provide additional employee training in the event that a performance issue related to compliance with this Policy or the Agent's anti-money laundering and anti-fraud policies or procedures is identified. Employees should be tested on their knowledge to demonstrate understanding of their compliance responsibilities.

4.4 Agents shall document and maintain all training records. These documents shall be kept in the employees' personnel files and/or in with the MoneyGram's Learning Management System, and be provided to MoneyGram or appropriate government authorities upon request.

5 COOPERATION WITH LAW ENFORCEMENT AND REGULATORS

MoneyGram partners with law enforcement around the world to pursue the arrest and conviction of those who try to engage in illegal activities using MoneyGram's products and services. In addition, MoneyGram and its Agents are subject to examination for compliance with laws, regulations, and with MoneyGram's policies and procedures by governmental authorities in many jurisdictions. Government regulators and law enforcement agencies may seek information and records from time to time.

5.1 Agents shall cooperate fully with MoneyGram and law enforcement and/or regulatory agencies when contacted about consumer fraud or anti-money laundering compliance matters to the maximum extent allowed by law. If responding to the request is beyond their ability, the Agent must promptly contact MoneyGram for assistance (see Important Contact Information).

5.2 Any person associated or connected with an Agent and who receives or is served a summons, subpoena, court order, or other formal inquiry related to MoneyGram's products, services or business shall immediately contact MoneyGram, if permitted by applicable law or regulation (see Important Contact Information).

5.3 Agents and their employees shall cooperate and respond promptly to all lawful requests for information including:

- any MoneyGram request for records or other information;



- any regulatory exam, inspection, independent testing or compliance review of the Agent's business; and
- any appropriate governmental request for records including subpoenas, production orders, or other requests related to the Agent's sale of MoneyGram's products and services.

6 TRANSACTIONS AND RECORDKEEPING REQUIREMENTS

The core of MoneyGram's products and services are the transactions it processes. It is necessary for Agents and their employees (when applicable) to gather complete and accurate information to ensure that MoneyGram transactions are processed correctly and efficiently. Agents and their employees (when applicable) gather various types of information throughout the transaction process, including not only documentary information, but also behavioral/nonverbal information from consumers (when transactions are conducted in person), such as body language and tone of voice. The information gathered and observed may be useful in preventing MoneyGram's products and services from being used for illegal purposes and may aid both MoneyGram and the Agent in fulfilling their anti-money laundering and anti-fraud obligations, including reporting suspicious activity. In addition, Agents shall follow the laws and regulations governing the retention of records associated with transactions, suspicious activity, and other regulatory reports.

- 6.1 Agents located in the United States, or with locations within the United States, shall maintain all records and reporting documentation required by the Bank Secrecy Act ("BSA") for a minimum of five (5) years (or longer if specified by a state specific regulation³) in a safe and secure location and make it readily available to the U.S. Treasury Department and/or representatives from other government officials upon lawful request.
- 6.2 Agents located outside of the United States, or with locations outside of the United States, shall maintain all transaction and consumer due diligence records to comply with information requests for five (5) years (or longer if required locally) as recommended by the Financial Action Task Force ("FATF") on Money Laundering.
- 6.3 Agents are required to maintain records that document their efforts to monitor, prevent, and report consumer fraud, money laundering, and terrorist financing for a minimum of five (5) years (or longer if required by local laws or regulations).
- 6.4 Agents and their employees should warn consumers prior to the completion of their transaction about current fraud "scams" by referencing the warnings on the send form (where applicable) or other relevant packaging for products.

³ In addition to the BSA, Agents located in the United States or with locations within the United States, shall maintain all records and reporting documentation required by the Electronic Funds Transfer Act ("EFTA") and Regulation E (also known as the Remittance Transfer Rule) for a minimum of two (2) years (or longer if specified by a state regulation) in a safe and secure location, including the Agent receipt / copy.



6.5 Agents and their employees shall ensure that:

- Where applicable, send and receive forms are filled out fully and accurately and signed by the consumer.
- Valid consumer identification information is obtained before the transaction is processed in accordance with local requirements and MoneyGram's policy and procedures.
- Complete and accurate consumer identification information is entered into MoneyGram's systems to ensure data quality and to minimize delays in processing the transaction.
- Transactions that appear unusual or possibly tied to money laundering or other illegal activities should be reported to the relevant authority as required by applicable laws or regulations and/or escalated to MoneyGram when appropriate.
- Consumers that appear to be involved in a fraud-induced transaction are questioned about their transaction. If there is a reasonable suspicion that the transaction is fraud-induced, the Agent or their employee shall refuse to process the transaction and report as soon as reasonably possible such activity to MoneyGram and the appropriate authorities, where required by applicable law or regulation.
- Consumers whom report to an Agent or their employee that they have been the victim of a fraud-induced transaction are encouraged to separately report fraud-induced transactions to MoneyGram and/or the appropriate authorities.

6.6 Before releasing the funds to the consumer, the Agent and their employees should request the reference number from the consumer and enter this number in MoneyGram's systems.

7 CONSUMERS RIGHTS

MoneyGram is committed to protecting its consumers from unethical or illegal business practices. MoneyGram expects that Agents and their employees minimize risk of harm to consumers, and prevent occurrences of unfair, deceptive, or abusive acts or practices ("UDAAP") or violations of other applicable consumer protection laws by all means reasonably practicable under laws and regulations.

7.1 Agents shall disclose all required information to consumers regarding each transaction, including information related to fees and what the consumer will be charged for each transaction.



- 7.2 Agents may only offer MoneyGram's product and services in languages approved and authorized by MoneyGram.
- 7.3 Agents may only use MoneyGram approved marketing materials and advertisements. These include internal and external signage, promotional pamphlets, advertisements in local periodicals, and counter-top displays.
- 7.4 MoneyGram's systems have been specifically configured to generate the types of pre-payment and post-payment disclosures required under the applicable laws and regulations, including the United States Remittance Rules. Agents may not make any changes to the pre-payment and post-payment disclosures provided by MoneyGram or generated from MoneyGram's equipment.

8 CONSUMER PRIVACY AND DATA PROTECTION

MoneyGram provides secure, convenient ways to send and receive money. Part of MoneyGram's commitment to its consumers is that it will safeguard their personal and private information. During the course of transactions, Agents and their employees may receive personal and private information from consumers such as name, address, phone number, government identification/ID or tax identification number, passport number, bank account number, credit or debit card number, place or date of birth, occupation, email address, and any other required consumer due diligence. MoneyGram expects that Agents and their employees protect this information from unauthorized access, use, and disclosure.

- 8.1 Agents shall protect consumers' personal and private information, in accordance with applicable laws and regulations, to prevent unauthorized access, use, and disclosure.
- 8.2 Agents' anti-money laundering and anti-fraud programs shall include procedures to comply with privacy laws and to ensure data security. Such procedures shall be implemented, commensurate with the type of information collected and stored and the business operations of the Agent.
- 8.3 Agents and their employees shall collect from consumers only the information needed to complete a transaction. Agents and their employees shall only use consumer information for identified and allowable purposes as provided in the terms and conditions contained in the documents given to consumers. Unless otherwise authorized by MoneyGram, consumer information can only be used (i) to complete a consumer transaction; (ii) to meet legal/regulatory obligations; and (iii) to prevent money laundering and/or fraud.
- 8.4 Agents shall disclose consumer information only to the individual whom it pertains, and shall not disclose consumer information to any unauthorized third party.



- 8.5 Agents shall retain consumer personal information for only as long as necessary to fulfill the stated purpose or as required by law. All documents that contain consumers' private and personal information shall be stored in a secure location. If an Agent uses tools to assist with transaction monitoring, it must follow appropriate data security protocols.
- 8.6 Agents shall ensure proper destruction of consumer personal information at the end of the retention period.
- 8.7 Agents shall ensure that each employee has an individual ID and password which are not shared among employees.
- 8.8 Agents and their employees shall refrain from and prevent use of MoneyGram's computer hardware, software, communications, and network systems for personal use or use unrelated to MoneyGram's business. Agents shall protect their Money Transfer computer against unauthorized access and should not use the Money Transfer computer for Internet browsing, emailing, or Instant Messaging (IM) as these are the most common methods for computers to become infected with viruses and/or phishing software that can lead to fraudulent transactions. Computer screens should not be visible to the public. Agents should install the appropriate anti-virus software and firewalls as well as configure the software to automatically download patches and upgrades to fix security holes.
- 8.9 Agents shall report any incident in which the confidentiality or security of any consumer personal information has been or is suspected to have been disclosed, misused, or compromised immediately to both the appropriate management at the Agent and to MoneyGram (see Important Contact Information) in order to determine the potential impact to the Agent, consumers, and MoneyGram.

9 CONSUMER REFUNDS

Occasionally errors are made when a transaction is processed. MoneyGram has instituted procedures to comply with the applicable laws and regulations, including the United States Remittance Rules that cover when a refund must be provided to a consumer. Agents should work with the consumer and MoneyGram to resolve any transaction errors. Moreover, MoneyGram expects its Agents to put forth all reasonable efforts to prevent disbursement of fraudulently induced transactions and issue refunds consistent with MoneyGram's procedures as well as local consumer protection laws.

- 9.1 If the Sender or Receiver believes that an error has occurred, contact MoneyGram immediately. MoneyGram will investigate the alleged error and determine if a refund is to be provided to the consumer.



9.2 Agents shall assist MoneyGram in providing refunds to consumers where applicable.

9.3 Agents shall advise the consumer to immediately contact MoneyGram if the consumer believes they have sent a fraudulently induced transaction, even if the Agent is unable to provide a refund to the consumer.

10 MONITORING AND CORRECTIVE ACTION

MoneyGram monitors how well Agents carry out their compliance responsibilities. This includes monitoring transactions processed by an Agent. In its discretion, MoneyGram conducts reviews of Agents' anti-money laundering and anti-fraud compliance programs, Mystery Shopping, Onsite Investigations, and other compliance review activities to ensure that the Agent has designed and implemented an effective compliance program tailored to the Agent's business model and that the Agent is following the applicable legal and regulatory requirements, MoneyGram's policies and procedures, and/or contractual requirements.

10.1 Conduct that Could Lead to Monitoring or Corrective Action

- All Agents who violate this Policy, or any applicable law or regulations shall be subject to immediate corrective or remedial action, including probation, suspension of service or termination of MoneyGram's services.
- MoneyGram may take corrective or remedial action, including probation, suspension of service or termination of MoneyGram's services, if it determines, in its sole discretion, that an Agent's conduct poses an undue risk to consumers or MoneyGram's reputation or systems. Conduct that may lead to corrective or remedial actions includes processing suspicious or fraudulently induced transactions.
- Any Agent found to assist or participate in illegal transaction activities will be subject to immediate suspension or termination of MoneyGram's services, absent documented mitigating circumstances.

10.2 Possible Monitoring and Corrective Actions

- MoneyGram may choose to take a variety of corrective or remedial actions to address the conduct set forth in Section 10.1 above. These actions may include:
 - termination of MoneyGram's services;
 - suspension of the right to conduct MoneyGram money transfer or other transactions;



- imposition of restrictions on MoneyGram’s services, including: (i) lowering of thresholds for consumer identification procedures; (ii) lowering of transaction volume or transaction amount limits; (iii) requiring express MoneyGram approval of transactions above a certain amount; and (iv) other restrictive measures deemed necessary by MoneyGram; and
- placing the Agent on a period of probation during which MoneyGram will closely monitor the Agent’s transactions. In instances where the Agent is placed on probation, the Agent’s MoneyGram transactions will be monitored for a period of 90 days or until such time as MoneyGram deems sufficient.
- Additionally, MoneyGram may undertake other remedial actions separately or in conjunction with those listed above in Section 10.2. These actions may include:
 - contacting the Agent every 30 days to receive reports regarding an Agent’s actions taken in response to identified issues;
 - requesting and reviewing the Agent’s documentation; and
 - addressing transaction analysis with the Agent every 30 days.

10.3 Agents shall respond to and implement all corrective or remedial actions required by MoneyGram to address violations or deficient adherence to this Policy. MoneyGram will terminate its services with Agents who fail to respond to or implement corrective or remedial actions required by MoneyGram.

10.4 Any Agent who believes it has been unfairly subjected to corrective or remedial action shall contact MoneyGram’s Chief Compliance Officer at:

MoneyGram International, Inc.
Attn: Chief Compliance Officer
2828 North Harwood Street, 15th Floor
Dallas, TX 75201
Phone: (+01) 214-999-7640

10.5 Corrective Actions Related to Agent Employees

- Agents shall investigate and report to the appropriate authorities and MoneyGram any instances where an employee is suspected of participation in money laundering, consumer fraud, or terrorist financing.



- Agents shall prohibit employees suspected of participation in money laundering, consumer fraud, or terrorist financing from performing MoneyGram transactions and remove the employee's access to MoneyGram's systems.
- If the Agent, upon investigation, believes an employee previously suspected of participation in money laundering, consumer fraud, or terrorist financing, did not actually participate in these activities, then the Agent shall obtain approval from MoneyGram before reinstating the employee's access to MoneyGram's systems.



IMPORTANT CONTACT INFORMATION

CHIEF COMPLIANCE OFFICER

Our compliance team is available at:

MoneyGram International, Inc.
 Attn: Chief Compliance Officer
 2828 North Harwood Street, 15th Floor
 Dallas, TX 75201
 Phone: (+01) 214-999-7640

Reason to Contact	MoneyGram Contact Information
<p>Hotline Agents and their employees have the ability to contact MoneyGram immediately by telephone to stop a fraud-induced transaction, or to file a confidential, anonymous report regarding ethics violations by telephone or email. This Hotline should be used in the following situations:</p> <ul style="list-style-type: none"> • Report a consumer transaction that appears to be fraud-induced, in progress and requires immediate attention. • Report violations by Agent or Agent Employees of MoneyGram’s Global Partner Compliance Policy’s Legal and Ethical requirements. • Report violations by MoneyGram or MoneyGram Employees of MoneyGram’s Global Partner Compliance Policy’s Legal and Ethical requirements. • Report instances where an Agent or their employee is suspected of participation in money laundering, consumer fraud, or terrorist financing. 	<p>Report Fraud PHONE in the United States 1-800-866-8800 outside of the United States http://corporate.moneygram.com/compliance</p> <p>Report Violations PHONE United States 1-800-866-8800 for English or Spanish</p> <p>ONLINE Complete the online form by visiting http://corporate.moneygram.com/compliance</p>
<p>Potentially Suspicious or Unusual Activity Escalation Agents and their employees have the ability to immediately report to MoneyGram information related to potentially suspicious or unusual activity, including suspected instances of consumer fraud.</p> <ul style="list-style-type: none"> • Report information related to potentially suspicious or unusual consumer activity, including activities attempted by consumers. • Report consumer transactions that appear to be fraud-induced and are no longer in progress. 	<p>PHONE United States 1-800-866-8800 for English or Spanish</p> <p>ONLINE Complete the online form by visiting http://corporate.moneygram.com/compliance</p>



Reason to Contact	MoneyGram Contact Information
<p>Law Enforcement or Regulatory Request Assistance Agents and their employees may contact MoneyGram regarding any questions regarding law enforcement or regulatory requests or inquiries.</p>	<p>EMAIL MGILEDirect@moneygram.com</p>
<p>Consumer Privacy and Data Protection Request Assistance Agents and their employees must contact MoneyGram immediately to report any incident in which the confidentiality or security of any consumer’s personal information has been or is suspected to have been disclosed, misused, or compromised.</p>	<p>EMAIL PrivacyProgramOffice@moneygram.com</p>
<p>General Agent Assistance Agents and their employees may contact MoneyGram to receive assistance or guidance regarding general topics, including:</p> <ul style="list-style-type: none"> • Consumer refund requests; • Technology or equipment support; • Request systems or compliance training; and • Any other questions not covered by the above provided contact information. 	<p>PHONE United States 1-800-444-3010 for English or Spanish</p> <p>AGENT CONTACT ME SERVICE <i>Web</i> https://www.callmoneygram.com/moneygram</p> <p><i>Phone</i> +1 720 362 5024 (there is no charge for this call)</p> <p>POWERTRANSACT CONTACT ME SERVICE <i>Web</i> https://www.callmoneygram.com/PwT</p> <p><i>Phone</i> +1 720 362 5025 (there is no charge for this call)</p> <p>ONLINE Complete the online form by visiting http://corporate.moneygram.com/compliance</p>