Global Anti-Money Laundering Policy

Master List Ref	Release Date	Review Date	Next Review Date
Fin-01.0-AML	June 2024	June 2024	January 2025
Version: **1.0**	**Process Owner** Finance	**Reviewed by** Legal & Compliance (Global)	**Approved by** SVP - Finance

Contents

Introduction and Purpose

Firstsource Solutions Limited and its subsidiaries ("**Firstsource**") service global clients across several business segments, including Banking, Telecom, Healthcare, Collections, Mortgage, Utility, Media, Communication, Education Technology and Insurance. For the purpose of this policy, Firstsource and its subsidiaries are collectively referred to as "Firstsource".

Firstsource is committed to carry out its business in accordance with the highest ethical standards and in compliance with all applicable laws, which includes complying with all applicable Anti-Money Laundering ("**AML**") laws and global AML standards in the conduct of its business and having a process to prevent any violations of such AML laws and global standards. To this effect, Firstsource conducts its business only with reputable parties who are involved in legitimate business activities.

This Anti-Money Laundering Policy ("**Policy**") is implemented by Firstsource with an objective of reducing the risk of money laundering and terrorist financing associated with its business and operations.

This Policy constitutes the minimum standard. Should there be any contradictions between this Policy and any applicable law in any country of Firstsource's business and operations, such law shall take precedence over this Policy.

Policy Coverage

This Policy is applicable to all Firstsource employees, officers, trainees, apprentices and interns ("**Firstsource Personnel**"), vendors, partners, clients, and third Parties in their dealings with Firstsource and with each other in relation to Firstsource's business.

Money Laundering

Money laundering is the concealment of the origins of illegally obtained money/ proceeds ("**illicit funds**") so that they appear to have originated from legitimate sources thereby avoiding prosecution, conviction and confiscation of such illicit funds. Laundered money may be used for terrorism and terrorist financing, tax evasion, drug trafficking, human trafficking, smuggling, bribery, and other illicit and criminal activities. by anyone who provides or receives such illicit funds. It is the process by which the identity of the illicit funds is changed so that it appears to come from a clean and legitimate source.

There are three (3) stages of money laundering:

1. **Placement:**

This is the first stage of money laundering where illicit funds which are acquired through theft, bribery, corruption and other illegal activities are placed into legal and financial systems in order to move such illicit funds away from their sources. It is where the illicit funds are 'washed' and disguised by being placed into a legitimate financial system, such as in offshore accounts. There are several ways to do this kind of placement, such as:

(a) *Blending of funds*: blending illicit funds with legitimate undertakings to avoid detection;
(b) *Invoice frauds*: over invoicing, under invoicing, falsely described goods and services, phantom shipping, etc.;
(c) *Smurfing*: breaking illicit funds into smaller and less-suspicious transactions below the reporting threshold by depositing such illicit funds into one or multiple bank accounts by multiple people (known as 'smurfs') or by a single person over a long period;
(d) *Offshore accounts for tax evasion*: placing illicit funds through offshore accounts, which easily hides the beneficial owners' identity to avoid paying tax;
(e) *Carrying small sums of illicit funds abroad*: carrying small sums of illicit funds abroad below the customs declaration threshold and then paying the illicit funds into foreign back accounts before sending it back to the country of its origin;
(f) *Aborted transactions*: transferring the illicit funds to a lawyer or accountant to hold until a proposed transaction is completed and then cancelled so that the illicit funds can be paid back to criminals from an unassailable source.

2. Layering

Layering is a significantly intricate element of the money laundering process. Its purpose is to separate illicit funds from their source and creating "layers" of multiple financial transactions to conceal the source and ownership.

This can include using multiple banks and accounts, having professionals act as intermediaries and transacting through corporations and trusts, and creating layers of complex financial transactions, such as converting cash into travellers' checks, money orders, wire transfers, letters of credit, stocks, bonds, or purchasing valuable assets, such as art or jewellery. These transactions are designed to disguise the so-called paper or audit trail and anonymize the launderers' identities.

3. **Integration**

The third and final stage of the money laundering process is called the integration stage during which, the illicit funds are returned to the launderer from what seem to be legitimate sources. The illicit funds become fully integrated into the financial system at this stage and can be used for any purpose, having been placed initially as cash and layered through several financial transactions. The objective is to have the illicit funds returned to the launderer in a manner that does not draw attention and appears to result from a legitimate source. Purchasing luxury goods such as upper-class property, artwork, jewellery, or high-end automobiles are common ways for the launderer to enjoy their illegal funds without drawing attention of the authorities.

Potential Red Flags

Compliance with AML and anti-terrorism laws and regulations requires awareness of potential "red flags" or suspicious activities, which may arise in the course of doing business. Each and every person associated with Firstsource including, but not limited to, all Firstsource Personnel, clients, vendors, third parties and investors are required to adhere to the legally compliant standards to protect Firstsource, its business and its reputation from being misused for money laundering or any other illegal financial activities.

Below are examples of potential red flags which Firstsource Personnel and representatives working on behalf of Firstsource with Firstsource's clients and vendors or potential clients and vendors, should be aware of. In the below examples "entities" mean organizations (profit and non-profit) and individuals who engage with Firstsource for its business or to provide goods and services to Firstsource:

(a) Entities belonging to or connected with countries which are identified as uncooperative or under the scrutiny for money laundering or considered to be "high risk for money laundering" by international organizations against money laundering and by the Financial Action Task Force (FATF).

(b) Entities reluctant to provide information about themselves or provide insufficient, false or suspicious information, especially with regard to their beneficial ownership.

(c) Entities unwilling to comply with Firstsource's policies related to anti-bribery/ anti-corruption, anti-money laundering, financial crime, etc.

(d) Entities acting on behalf of another organization or individual but refusing to provide or are reluctant to provide complete information regarding such other organization or individual or provide insufficient, false or suspicious information.

(e) Entities paying or asking for payments in modes which are inconsistent with the payment policies of Firstsource, and/ or which are not customarily used in the ordinary course of business. Examples of such modes are payments with money orders, travellers' checks, multiple negotiable instruments to various parties for one transaction, payments to or from unrelated third parties, payment in cash or etc.

(f) Orders or purchases that are inconsistent with Firstsource or the entities' trade or business

(g) Payments to or from countries which are considered to be "high risk" for terrorist financing and/ or considered to be tax havens or offshore jurisdictions

(h) Overpayments followed by directions to refund such payment or a portion thereof, for example, paying by credit card and requesting a wire transfer or cash refund.

(i) Structuring transactions to avoid government reporting or record keeping requirements

(j) Entities having unusually complex business structures or payment patterns.

(k) Entities providing addresses which are not a physical site.

(l) Entities involved in "vulnerable transactions" as defined by applicable law.

Compliance Controls

Firstsource ensures that its business has a culture of compliance and effective controls to comply with AML laws and regulations to prevent and detect money laundering activities and terrorism financing. To this effect, all designated Firstsource Personnel who are liaising with Firstsource's clients, vendors and other third parties for Firstsource's business and operational purposes shall be responsible for ensuring that this Policy is being complied with. The following steps shall be undertaken by Firstsource Personnel in their transactions with Firstsource's clients, vendors and third parties:

1. *Due diligence*: Firstsource Personnel shall conduct due diligence in accordance with Firstsource policies and standards and be familiar with the business practices of vendors and third parties that engage with Firstsource, including the nature of the particular goods of services being provided as some transactions are more likely to give rise to a risk of money laundering. This shall include sanctions screening and may include adverse media and politically exposed persons ("PEP") screening.

2. *Monitoring financial activities*: Firstsource Personnel shall observe and record payments and transactions consistent with Firstsource policies and global financial standards.

3. *Record Keeping and Retention of Records*: Firstsource Personnel shall keep current, complete and accurate records of every business transaction of Firstsource. Records confirming the identity of clients, vendors, third parties, investors and other persons engaging with Firstsource shall be retained for periods as prescribed in applicable laws and in accordance with Firstsource policies on document retention.

4. *Imparting Awareness about AML standards*: Designated Firstsource Personnel shall be aware of applicable AML standards and applicable laws, policies and procedures; and have a system of internal checks reasonably designed to ensure ongoing compliance with this Policy, applicable AML standards, laws, other financial policies and procedures for receipt and provision of goods and services.

Policy violations and Reporting of money laundering activities:

Violations of this Policy include the following actions by Firstsource Personnel:

1. Violations of the AML compliance controls

2. Engaging with clients, vendors and third parties in contravention of this Policy and other applicable policies of Firstsource

3. Instigating other Firstsource Personnel and/ or clients, vendors and third parties to violate this Policy in relation to Firstsource's business

4. Failure to raise a known or suspected violation of this Policy or report a red flag or any suspicious transaction related to Firstsource's business

5. Failure to comply with investigation into actual or potential violations of this Policy

6. Involvement in any form of money laundering activities, whether in the course of employment at Firstsource or otherwise.

Any violations to this Policy must be reported immediately to the Legal Department of the related geography or at whistleblowing@firstsource.com. Failure to do so will result in disciplinary proceedings and any other action that Firstsource deems fit, in accordance with applicable Firstsource policies and laws. Any breach of this Policy by a vendor will lead to Firstsource terminating the contract with the vendor and seeking remedies under law for

damages, if any. Any breach of this Policy by a third party desirous of engaging with Firstsource, may result in such third party's business proposal being rejected by Firstsource.

The Legal Departments, in conjunction with Firstsource leadership, will determine whether government reporting is necessary based on the information collected during any AML-related investigation. Such reporting may include the filing of suspicious activity reports or other similar documentation, depending on the requirements of applicable laws in the specific country.

Applicability for UK and North America

In addition to the contents of this Policy:

a. The UK's Financial Crime Policy, available at Microsoft Word - Financial Crime Policy - V4.2.docx (firstsource.com) details the specific geographic provisions for the UK.

b. Specific provisions contained the Bank Secrecy Act and Anti-Money Laundering Policy is available at https://www.firstsource.com/wp-content/uploads/2023/11/Bank-Secrecy-Act-and-Anti-Money-Laundering-Policy.pdf shall apply to specific North American entities, including those in the United States and Mexico.

Review of this Policy

This Policy is continually evolving. This Policy neither can, nor intends to, encompass every situation. This Policy may undergo changes based on business requirements and changes in law and regulations from time to time.