Flywire Corporation Global Anti-Money Laundering (AML) /Counter-Terrorist Financing (CTF) Compliance Program Overview

Flywire Corporation | 141 Tremont Street, Boston, MA 02111

v.2 January 2024

Table of Contents

Introduction

Flywire Corporation through its subsidiaries[1] (collectively Flywire) is registered as a licensed payments company or Money Service Business ("MSB") in the European Union (via our passported Lithuanian license), the UK, the US, Canada, Australia, New Zealand and Singapore. Therefore, Flywire is subject to a diverse set of regulatory requirements across these various jurisdictions. In addition to its geographic diversity, Flywire is exposed to market diversity via its processing of international and domestic payments in its education, health care, travel, and business-to-business ("B2B") verticals. Flywire does not engage in processing transactions in cash, nor do we serve customers in the gaming, adult industry, cannabis or virtual currency/asset sectors (among others).

This document summarizes the steps Flywire takes to maintain its global compliance program. Flywire does not have a "one-size-fits-all" compliance program and tailors its procedures to comply with local requirements. Flywire will not knowingly violate compliance or regulatory requirements in any jurisdiction and aspires to follow not just the letter, but also the spirit of the law.

As a publicly traded corporation (Nasdaq Global Select Market: FLYW) headquartered in the United States, Flywire through its global subsidiaries maintains a compliance program designed to comply with The Financial Recordkeeping and Reporting of Currency and Foreign Transactions Act of 1970 (The Bank Secrecy Act) ("BSA") and global financial crimes compliance requirements of the jurisdictions in which Flywire operates. The BSA and other global regulations (collectively, the "AML Laws") require financial institutions to identify and report potential money-laundering activities, terrorist financing, illegal activities, and certain other suspicious transactions conducted by or through the business. The AML Laws also require Flywire entities to make and retain certain records regarding customers, transactions and accounts. Flywire has implemented the standards set forth by the Financial Action Task Force ("FATF") in each of the jurisdictions in which the company operates, along with any local standards that go beyond the FATF standards.

[1] This Financial Crimes Compliance overview describes the program applicable to Flywire Corporation and its subsidiaries including but not limited to: Flywire Payments Corp (US); Flywire Global Corp (US); Flywire Payments Canada, Inc.; Flywire Payments Ltd (UK); Flywire Europe, UAB; Flywire (Singapore) Pte. Ltd; and Cohort Go.

The Compliance Program

Flywire's AML/CTF Program includes, but is not limited to, the following core components:

1. Policies and Procedures that document AML/CTF Program requirements;
2. A designated person to oversee compliance with the AML/CTF Program;
3. Periodic independent review of the AML/CTF Program;
4. Know Your Customer (KYC) Program;
5. Training of appropriate personnel about their responsibilities under the AML/CTF Program;
6. Governance;
7. Financial Crimes Compliance Risk Assessment and maintenance of a risk register;
8. Government Sanctions Screening;
9. Transaction Monitoring;
10. Regulatory Reporting;
11. Fraud Monitoring Program, and;
12. Recordkeeping

1) Policies Procedures and Internal Controls

In the jurisdictions in which Flywire conducts business, regulations require covered financial institutions to establish written, risk-based, AML programs reasonably designed to prevent the business from being used to facilitate criminal activity. Flywire maintains policies and procedures and internal controls that govern the AML/CTF program globally and locally. Where necessary, local procedures are implemented to supplement the global program to ensure that Flywire complies with local AML Laws. Although local procedures are developed and managed in-country by regional compliance managers, the local processes may be executed in other countries. Some compliance functions at Flywire operate in a similar manner by leveraging the expertise of global employees along with the oversight and approval by in-country compliance personnel. This model allows Flywire to standardize compliance processes across the company while complying with local laws ensuring a minimum standard of compliance oversight in every jurisdiction in which Flywire operates.

2) Compliance Officer

To have an effective Financial Crimes Compliance program, Flywire entities name a person with sufficient knowledge to serve as [a regional] compliance officer or money laundering reporting officer ("MLRO") and provide said person adequate resources. This serves as a pillar of an effective compliance program.

Flywire's Chief Compliance Officer ("CCO") is responsible for management and supervision of the AML/CTF program. The CCO function possesses the necessary resources to effectively implement and maintain Flywire's AML/CTF Program, as well as the necessary independence and authority to do so. The CCO also fosters a culture that addresses compliance concerns in a prompt and appropriate manner. The responsibilities of the CCO include, but are not limited to, the following:

- Ensuring Flywire's AML/CTF Program is updated as necessary to reflect changes in the applicable laws, regulations, and guidance;
- Ensuring resources are properly allocated and that material elements of Flywire's AML/CTF Program are effectively implemented;
- Ensuring regulatory reports are filed, and records are retained in accordance with applicable law;
- Responding to any law enforcement requests with assistance of counsel as necessary;
- Coordinating with and responding to examiners during regulatory reviews;
- Ensuring appropriate national, international and local registration and licenses (if required) are properly maintained;
- Ensuring appropriate ongoing independent review of Flywire's compliance program (in jurisdictions where appropriate);
- Ensuring appropriate AML/CTF training and education is provided to employees and;

- Reporting to senior management and Flywire's Board in a timely and ongoing manner regarding material changes to Flywire's AML/CTF Program, including but not limited to reporting material changes with respect to: new regulatory requirements; implementation of material new initiatives; material AML compliance issues (e.g., identified risks that may not be fully mitigated by existing AML procedures); the results of audits, internal reviews, and regulatory examinations; changes to the AML risk profile; significant suspicious activity reports ("SARs")[2] ; and any material issues with regulatory authorities.

While the CCO retains overall responsibility for the AML/CTF Program, he or she may delegate the responsibility for management and oversight of the AML/CTF Program as he or she deems appropriate. This may include delegation to other Flywire departments and employing and empowering regional compliance directors in the Americas, EMEA and APAC to facilitate both full time responsiveness and regional expertise.

3) Periodic Independent Review

A Periodic Independent Review is another pillar of an effective Financial Crimes Compliance program. Flywire conducts an independent review of its AML/CTF Program– engaging a prominent third-party auditor – at least every 2 years where regulation permits or more frequently, typically annually. The review and audit testing includes: (1) a test of internal procedures (2) a review of transactions monitoring and reporting (3) a test of the record keeping system (4) an analysis of whether the designated compliance officer(s) have performed adequately and (5) documentation of the scope of the testing procedures performed. The periodic Independent Review is shared annually with Flywire's Board of Directors, which, along with the designated compliance officers, are charged with addressing any findings or recommendations.

The independent review results can be shared with banks/financial institutions used by Flywire as part of proactively managing Flywire's vital banking relationships, when appropriate. Flywire has an independent auditor review its operations in the U.S., the E.U., the U.K., Canada, Australia, and New Zealand.

Flywire will also complete periodic Independent Reviews where Flywire obtains licenses in new jurisdictions.

[2] The acronym "SAR" is utilized throughout this document and is interchangeable with other global suspicious activity reporting acronyms, such as STR or SMR

4) Know Your Customer (KYC): Including Politically Exposed Persons (PEPs) and Underlying Beneficial Ownership (UBO)

As part of meeting its Financial Crimes Compliance requirements, Flywire also maintains a KYC program, to ensure that clients are who they claim to be, and are not subject to sanctions, or other limitations/prohibitions on sending or receiving payments. Following best practices, Flywire gathers appropriate information prior to establishing a customer account. Flywire will obtain information designed to verify the existence of the entity, the products and services provided by the entity, the ownership and executive officers, verification against global sanctions lists, commercial credit and references, bank accounts, a background check of the website, and other desk-based diligence checks (e.g., media reports), and may complete a site visit. For certain high-risk businesses, Flywire performs additional due diligence (sometimes referred to as “enhanced due diligence”) which may include, three prior months of bank statements, the balance sheet and income statement, credit history, current credit card or ACH processing statements, a bank reference letter, and commercial references. To the extent that information provided by the potential customer is incomplete, inaccurate or inconsistent, Flywire may request additional documentation or answers to questions intended to clarify matters related to the business and purposes of the payments (among other matters).

Additionally, Flywire will collect information including any necessary enhanced due diligence for Politically Exposed Persons (“PEPs”) and their close associates.
Flywire does so to mitigate the risk of enabling corruption. These precautions are not designed to prevent PEPs from opening accounts, rather, they help determine the level of risk involved.

Flywire mitigates the risks that PEPs present in a number of ways, including by identifying the beneficial owners of the relevant legal entities, by engaging in direct information gathering from the account holder and beneficial owners, by conducting adverse media research, by verifying employment, and country of residence, and by identifying the purpose of the account. When a PEP match is identified, the designated compliance officer or delegate reviews the account relationship and analyzes the relevant risks to determine if Flywire will continue or begin its relationship with the PEP.

At the time of opening an account for a legal entity customer, Flywire identifies any Underlying Beneficial Owners who directly or indirectly own 25% or more of the equity interests of the legal entity customer, and any individual with significant responsibility to control, manage, or direct a legal entity customer. If no one owns 25% or more of the relevant entity, Flywire may analyze the controllers or managers of the entity, as it seeks to replace the information otherwise gathered in the beneficial ownership analysis. To ensure uniform global high standards, Flywire seeks to be over inclusive when requesting and collecting information on beneficial ownership. Flywire also employs what are known as adverse media screens on beneficial owners or controllers, as applicable, using keyword(s) searches designed to elicit potential negative history from those individuals.

If Flywire cannot verify the identity of the person or entity seeking to become a Flywire customer, Flywire has procedures that help determine whether the account will open, the terms of use upon opening an account, when to close the account, and when to file a SAR, if necessary, to comply with local regulations.

After onboarding customers, Flywire will perform risk-based monitoring and ongoing monitoring, and if necessary, take corrective action up to terminating the relationship. Flywire may terminate the relationship if increased risk or contract non-performance occurs from the customer and prior notifications of concerns and failed remediation are not addressed. Throughout the course of a customer relationship, Flywire will periodically "re-KYC" clients if there is a change in ownership, account settlement or otherwise, to comply with regulations or the reasonable requirements of its banking partners.

5) Training

Compliance training is also one of the pillars of Flywire's effective Financial Crimes Compliance program. As a licensed payments company Flywire is required to have an initial and ongoing employee-training program reasonably designed to ensure the business meets its responsibilities under international regulatory regimes, and to make staff aware of the obligations the business has to adhere to comply with applicable laws

Flywire requires its employees to complete new hire AML Compliance/CTF/Fraud training as well as annual continuing education training as part of its Global AML Compliance Employee Training Program.

AML Compliance/CTF/Fraud training is made available through Flywire's internal learning management system and is mandatory for all employees. Employees have 30 days from the date of assignment to complete assigned training modules.
Training consists of: (i) an overview of relevant rules and regulations; (ii) a discussion of AML, sanctions, and fraud typologies; (iii) real-life examples/case studies; and (iv) scenario-based training. Employees must successfully pass the knowledge check portion of the training to complete the course. Flywire manages the training to 100% completion. Employees who do not complete the required training will be escalated to senior management. Failure to complete the required training may result in disciplinary action.

6) Governance

In order to ensure that decisions relating to Flywire's AML/CTF Program are appropriately vetted, Flywire implements and maintains a governance program comprised of Flywire Corporation and operating entity level boards of directors and oversight committees that review and approve updates or changes to the AML/CTF Program. Material updates to the Flywire AML/CTF Program Policies are implemented only after review and approval is provided by the appropriate governance committee or board of directors.

7) Risk Assessment

Above all, Flywire's program is risk based; designed to address the risk of money laundering and terrorist financing that is specific to Flywire. Flywire has completed and maintains a written AML/CTF Risk Assessment. The Risk Assessment is reviewed and updated approximately annually or is triggered upon promulgating any significant changes to products, services, customers or geography. Any changes to assessed risks may then result in necessary changes to the compliance program. In accordance with best practices and industry standards, the compliance officer submits the documented assessment and written compliance program to the Board approximately annually for review and approval / reaffirmation. Upon Board approval / reaffirmation, the designated compliance officer will appropriately communicate with and train staff on any changes to the program. The documented risk assessment is maintained by the designated compliance officer and available for review by regulators and banking or other business partners as needed.

8) Government Sanctions Screening

Flywire complies with economic sanctions laws and regulations in the jurisdictions it operates, including the economic sanctions administered and enforced by the US Department of the Treasury's Office of Foreign Assets Control ("OFAC"), the United Nations, the European Union, and the UK's Office of Financial Sanctions Implementation ("OFSI"), and other sanctions regimes as applicable. These regulations prohibit, among other things, providing services, or engaging in transactions with, individuals or entities targeted by applicable sanctions programs (sanctioned persons). To comply with sanctions regulations, Flywire refuses to onboard sanctioned persons as customers, refuses to process transactions involving sanctioned persons, and ensures that funds in Flywire's possession or control in which a sanctioned person has an interest are frozen ("blocked") or rejected and reported to the relevant authorities according to regulatory requirements. All clients (including their beneficial owners) are screened against applicable sanctions lists prior to establishing a business relationship and on an ongoing basis. Similarly, payors are screened real-time against applicable sanctions list[3]. In the event a potential sanctions match is identified, transactions are systematically paused and reviewed by Flywire's Compliance personnel for further adjudication.

As a matter of policy, Flywire prohibits activity involving individuals, entities, or partners that are in countries that are subject to comprehensive sanctions. At present, the countries subject to comprehensive sanctions are:

- Cuba
- Iran
- North Korea
- Syria

[3] Flywire utilizes LexisNexis to complete sanctions screening.

- The Ukrainian territories of Crimea, Luhansk People's Republic (LNR) and Donetsk People's Republic (DNR.

In addition, Flywire does not process payments involving the Republic of Sudan, the Russian Federation, and the Republic of Belarus.

9) Transaction Monitoring

Flywire maintains risk-based transaction activity monitoring. Following its KYC onboarding process, Flywire uses a third-party system[4] to monitor payor transactions involving the customer. The transaction monitoring system is designed to identify transactions that appear to be: (1) complex; (2) unusually large; (3) part of an unusual pattern of transactions; and/or (4) appear to have no apparent economic or visible lawful purpose.

The transaction monitoring system, using parameters that Flywire sets, monitors the: (1) volume; (2) velocity; and (3) value of transactions. For example, the system generates an alert: (1) when the volume of the transactions exceeds a specified number and/or USD limit in a day; (2) when a specified number of payments are completed over a specified time period; or (3) when there is a cumulative value over a specified USD limit attributed to a single payor annually. Flywire periodically reviews its transaction monitoring business rules and changes them as AML/CTF risk dictates. In certain instances, enhanced procedures and business rules can be in place for certain transactional and regional combinations.

Flywire has a multi-level system for monitoring alerts. Upon receiving an alert, Level 1 reviewers examine the alert and evaluate whether it should be escalated to Level 2. When alerts are escalated to Level 2, the Level 2 reviewer evaluates the escalated alert to determine whether to file a SAR. Flywire maintains sufficient records to enable transactions and activity in customer accounts to be reconstructed, if necessary, in compliance with the relevant regulatory requirements.

10) Regulatory Reporting

As part of Flywire's AML/CTF program, and as part of its Financial Crimes Compliance, and fraud monitoring functions, Flywire maintains a Regulatory Reporting program ("Reporting Program"). The Reporting Program provides guidelines for filing Regulatory Reports required by various governments around the world. The method and frequency of reporting varies based on local requirements.

Reportable transactions, including suspicious transactions, are reported in accordance with applicable AML Laws. Any reasonable suspicion of money laundering activity is required to be reported to the designated Compliance Officer under internal Flywire policy. Flywire also maintains an internal reporting system through which any employee may

[4] Unit 21

report suspicious activity without retaliation.

Flywire does not accept, transport or receive physical currency. Therefore, although Flywire is aware of the requirement to file Currency Transaction Reports in the United States for cash transactions of greater than $10,000 USD (and similar requirements in other jurisdictions), these requirements do not apply to Flywire's business.

11) Fraud Monitoring Program

Flywire's Fraud Monitoring Program is designed to prevent, detect, and report fraud-induced payments. The Fraud Monitoring Program focuses on awareness, fraud monitoring, fraud controls, and ongoing collaboration with law enforcement, financial institution partners and consumer advocacy organizations. The program is supported by the core compliance processes at Flywire along with a third-party Artificial Intelligence (AI) model[5] designed to continuously learn from past data to alert for bad behavior. Further, evaluations are completed by Flywire compliance staff and customers/payors who exhibit patterns of bad behavior, may be interdicted.

12) Recordkeeping

Flywire retains records for a minimum of five years after an account is closed and will include the following in the record: identifying information, a description of documents relied upon, methods to verify identity of the customer, and resolutions of any discrepancies. Should a prospective customer be declined, Flywire will retain the documentation for a minimum of seven years to help ensure any future applications are reviewed in light of the past application. Records and documents for Flywire's AML/CTF Program are retained according to, at a minimum, the period required by applicable law or regulation for the jurisdiction Flywire.

[5] Sift Science