EXCHANGE ANALYTICS
Regulatory Compliance Solutions

Anti-Money Laundering Awareness for Money Service Businesses (MSBs) Training Course 2024

Course Outline and Provider Qualifications

This is a **Role-Based Learning** Course designed to optimize your learning experience by tailoring the course contents to one of two categories of roles at financial service firms. Select the **Front Office Path** if you work in a sales, broker, trader or customer-facing role at your firm. Select the **Supervisory or Back Office Path** if you supervise personnel or work in any non-front office role, such as: finance, customer accounts, operations, compliance, legal, security or related roles. This path is also beneficial if you simply want to receive more comprehensive AML training.

Front Office Path

I. How Does Money Laundering Work?
   a. Placement
   b. Layering
   c. Integration

II. Regulatory Landscape
   a. What is Money Laundering and Terrorist Financing?
   b. International Efforts to Prevent Money Laundering and Terrorist Financing
   c. The Financial Action Task Force
      i. List of AML Deficient Countries
      ii. “Grey List” of Jurisdictions Under Increased Monitoring
      iii. “Black List” of High-Risk Jurisdictions
      iv. Statement on the Russian Federation
      v. Guidance on Crowdfunding as Impacted by Terrorist Groups
      vi. The Use of Crowdfunding to Raise Money for Terrorism
      vii. Guidance Regarding the Abuse of Non-Profit Organizations by Terrorist Groups
   d. Monitoring Government Sanctions Lists
   e. Jurisdiction Specific Content:
      - U.S.
         - U.S. AML - CFT Priorities
         - OFAC Sanctions Compliance
         - Digital Virtual Assets

- Australia Requirements
- Canadian Requirements
- European Union Requirements
- Hong Kong Requirements
- Japan Requirements
- New Zealand Requirements
- Singapore Requirements
- U.K. Requirements

III. AML Compliance Program Requirements
   a. Elements of an AML Compliance Program – Five Pillars
   b. Customer Identification Program Steps
   c. Suspicious Activity Reporting & Requirements
   d. SAR Requirements for MSBs
      i. Role of Individuals
      ii. Confidentiality
      iii. Records Retention
   e. Willful Blindness or Turning a Blind Eye
   f. Individual Liability
   g. Recommendations for Maintaining an Effective AML Compliance Program

IV. MSB Red Flags
   a. How Do You Recognize Money Laundering?
   b. MSB Common Red Flags
   c. FAFT Digital Asset Red Flags
   d. Red Flag Summary

V. Enforcement Cases
VI. MSB Case Study
VII. Quiz

Back Office Path

I. How Does Money Laundering Work?
   a. Placement
   b. Layering
   c. Integration

II. Regulatory Landscape
   a. What is Money Laundering and Terrorist Financing?
   b. International Efforts to Prevent Money Laundering and Terrorist Financing

c. The Financial Action Task Force
    a. List of AML Deficient Countries
    b. FATF “Grey List” of Jurisdictions Under Increased Monitoring
    c. “Black List” of High-Risk Jurisdictions
    d. Statement on the Russian Federation
    e. Guidance on Crowdfunding as Impacted by Terrorist Groups
    f. The Use of Crowdfunding to Raise Money for Terrorism
    g. Guidance Regarding the Abuse of Non-Profit Organizations by Terrorist Groups
d. The Egmont Group
e. Monitoring Government Sanctions Lists
f. Jurisdiction Specific Content:
    - U.S. Requirements
        - U.S. AML - CFT Priorities
        - OFAC Sanctions Compliance
        - Digital Virtual Assets
        - OFAC & Ransomware Payments
    - Australia Requirements
    - Canadian Requirements
    - European Union Requirements
    - Hong Kong Requirements
    - Japan Requirements
    - New Zealand Requirements
    - Singapore Requirements
    - U.K. Requirements

III. AML Compliance Program Requirements
    a. AML Program Elements - Five Pillars
    b. Customer Identification Program Steps
    c. Suspicious Activity Reporting & Requirements
    d. SAR Requirements for MSBs
        i. The Role of Individuals
        ii. Confidentiality
        iii. Crypto Currency
        iv. Records Retention
    e. Reporting Suspicious Cyber Activity
    f. Additional SAR Requirements
    g. Willful Blindness or Turning a Blind Eye
    h. Individual Liability
    i. Avoid Program Deficiencies Flagged by Regulators
    j. Recommendations for Maintaining an Effective AML Compliance Program

Provider Qualifications - About the Author

Joseph Adamczyk served as author. Prior to his affiliation with Exchange Analytics, he served as the Chief Compliance Officer for Options Clearing Corporation (OCC). Mr. Adamczyk oversaw the firm's compliance risk monitoring and governance programs, advised the board of directors and staff on compliance and regulatory requirements, and interacted with federal regulators on compliance, risk, and examination matters. Before joining OCC, Mr. Adamczyk worked at CME Group where he served as the Managing Director & Associate General Counsel overseeing the company's non-U.S. legal staff and activities. In this role, he interacted with regulators from around the globe. He also handled CME Group's interactions with U.S. regulators and other authorities on cybersecurity and technology controls, requirements, cyber incident response, and examinations.

At CME Group, Mr. Adamczyk also served as the Global Head of Investigations and Enforcement in the Market Regulation Department. In that role, he oversaw teams responsible for monitoring, investigating, and enforcing the CME Group exchanges' trade practice rules and other requirements. Mr. Adamczyk received his MBA from the University of Chicago, law degree from Loyola University Chicago School of Law, and undergraduate degree from DePaul University. He has no regulatory actions or other disciplinary history.