

Anti-Money Laundering Awareness Training Course 2023

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 **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 (Slides 1 through 63)

- 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
 - d. FATF List of AML Deficient Countries, Jurisdictions Under Increased Monitoring, & High-Risk Jurisdictions
 - e. Monitoring Government Sanctions List
 - f. Jurisdiction Specific Content: Canada, EU, Singapore, U.K., U.S.
 - g. Singapore Requirements
 - h. U.K. Requirements
 - i. European Union Requirements
 - Customer Diligence
 - Enhanced Diligence
 - Outsourcing
 - Beneficial Ownership
 - Reporting Obligations
 - Single EU Supervisor
 - Int'l Cooperation
 - Virtual Transfers

- j. Canadian Requirements
- k. FinCen AML/CFT National Priorities
- l. OFAC Sanctions Compliance
- m. Digital (Virtual) Assets
- III. AML Compliance Program Requirements
 - a. Elements of an AML Compliance Program – Five Pillars
 - AML Program Development
 - Annual Training
 - AML Compliance Officer
 - Testing
 - Customer Due Diligence
 - b. Customer Identification Program Steps
 - Obtaining Customer Identification Information
 - Verifying Customer Identification Information
 - Obtaining Additional Verification as Required
 - Maintaining Customer Identification Records
 - c. Suspicious Activity Reporting & Requirements
 - d. Willful Blindness or Turning a Blind Eye
 - e. Individual Liability
 - f. Recommendations for Maintaining an Effective AML Compliance Program
- IV. Red Flags
 - a. How Do You Recognize Money Laundering?
 - b. Common Red Flags
 - c. FAFT Digital Asset Red Flags
 - d. Red Flag Summary
- V. Enforcement Cases
 - a. Regulatory Cases – Common Characteristics
 - b. Regulatory Cases – 10 Case Summaries
- VI. Case Study
 - a. Case Study Knowledge Check
- VII. Quiz
- VIII. Acknowledgement

Back Office Path (Slides 1 through 83)

- 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
 - d. FATF List of AML Deficient Countries, Jurisdictions Under Increased Monitoring, & High-Risk Jurisdictions
 - e. The Egmont Group
 - f. Monitoring Government Sanctions List
 - g. Jurisdiction Specific Content: Canada, EU, Singapore, U.K., U.S.
 - h. Singapore Requirements
 - i. U.K. Requirements
 - j. European Union Requirements
 - Customer Diligence
 - Enhanced Diligence
 - Outsourcing
 - Beneficial Ownership
 - Reporting Obligations
 - Single EU Supervisor
 - Int'l Cooperation
 - Virtual Transfers
 - k. Canadian Requirements
 - l. FinCen AML/CFT National Priorities
 - m. OFAC Sanctions Compliance
 - n. Digital (Virtual) Assets
 - o. OFAC & Ransomware Payments
- III. AML Compliance Program Requirements
- a. AML Program Elements - Five Pillars
 - AML Program Development
 - Develop A Policy Statement
 - Procedures and Controls for Detecting and Reporting Suspicious Activity
 - Implementation of a Customer Identification Program (CIP)
 - Due Diligence and Monitoring
 - Training
 - AML Compliance Officer
 - Testing
 - Customer Due Diligence
 - b. Customer Identification Program Steps
 - Obtaining Customer Identification Information
 - Verifying Customer Identification Information
 - Obtaining Additional Verification as Required
 - Maintaining Customer Identification Records
 - c. Suspicious Activity Reporting & Requirements

- d. Reporting Suspicious Cyber Activity
 - e. Additional SAR Requirements
 - f. Willful Blindness or Turning a Blind Eye
 - g. Individual Liability
 - h. Avoid Program Deficiencies Flagged by Regulators
 - i. Recommendations for Maintaining an Effective AML Compliance Program
- IV. Red Flags
- a. How Do You Recognize Money Laundering?
 - b. Common Red Flags
 - c. FAFT Digital Asset Red Flags
 - d. Red Flag Summary
- V. Enforcement Cases
- a. Regulatory Cases – Common Characteristics
 - b. Regulatory Cases – 10 Case Summaries
- VI. Case Study
- a. Case Study Knowledge Check
- VII. Quiz
- VIII. Acknowledgement

Provider Qualifications - About the Authors

Joseph Adamczyk served as a co-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.

Megan Conley served as a co-author. Ms. Conley joined Exchange Analytics in August 2020. Previously she worked in CME Group's Washington, D.C. office, where she was responsible for advising on regulatory and legislative developments impacting the derivatives industry. Ms. Conley also spent time working in London on CME Group's integration with NEX and Brexit contingency planning. She began her career in Chicago working as an investigator in CME Group's Market Regulation Department where she specialized in money pass investigations and conducted a variety of trade practice program reviews. Ms. Conley is admitted to practice law in Illinois.