Basic Questions on AML

YouTube Channel Link: https://www.youtube.com/@Aml_Transformations

1.What is the purpose of AML and KYC regulations?

Answer)

AML (anti-money laundering) is an umbrella term for the range of measures, controls, and processes that firms must put in place in order to achieve regulatory compliance.

Anti-Money Laundering regulations are in place to mitigate the risk of money laundering and terrorism financing. Financial institutions are required to monitor their clients to prevent money laundering and report any financial crime they detect to relevant regulators.

KYC is a component part of AML, and refers specifically to the means by which firms establish and verify their customers' identities, and monitor their financial behaviour. Typically, the KYC process involves the collection and verification of a range of identifying information from customers including:

• Name

• Address

• Date of birth

Purpose of AML and KYC regulations:

AML (Anti-Money Laundering) and KYC (Know Your Customer) regulations are crucial components of financial oversight and risk management, these designed to prevent and combat illegal financial activities.

Federal Reserve is an important entity in the United States as RBI in India, AML and KYC regulations are typically overseen by various regulatory bodies, including the Financial Crimes Enforcement Network (FinCEN).

AML (Anti-Money Laundering) Purpose:

- Detect and prevent the conversion of illegally obtained funds (from activities such as drug trafficking, corruption, or fraud) into legal assets
- Identify and prevent the flow of funds to support terrorist activities.
- Protect financial institutions from being unwittingly involved in illegal financial transactions, safeguarding their reputation and stability.

KYC (Know Your Customer) Purpose:

- Verifying the identity of customers to ensure that financial institutions are dealing with legitimate individuals or entities.
- Understanding their customers, financial institutions can assess the risk associated with each customer and tailor their services
- Preventing identity theft and fraud by confirming the authenticity of customer information.

2. How do you verify a customer's identity during the onboarding process?

Answer)

1.Document Verification:

Requesting customers to upload a photo or scanned copy of government-issued identification, such as a driver's license or passport or state issued ID. This helps establish their identity.

Few examples of document verification methods:

- OCR-Based Verification:
  Leveraging Optical Character Recognition (OCR) technology to extract and verify information from identity documents.
- Image Authentication:
  Authenticating images of government-issued ID documents with Government Website.

2.Biometric Authentication:

Implement facial recognition technology to match a selfie taken by the customer with the photo on their government-issued ID.

3. Video Verification:

Live video calls with customers where they can display their ID and answer identity verification questions in real-time.

4.Two-Factor Authentication (2FA):

SMS or email verification as part of a two-factor authentication process, sending a one-time code to the customer's registered mobile number or email address.

3. What are some red flags that could indicate potential money laundering activity?

Answer)

Red flags indicating potential money laundering activity:

- Unusually large transactions or a series of transactions that exceed typical patterns could signal money laundering.
- Attempts to evade reporting requirements through structuring or layering transactions may indicate illicit financial activities.
- Funds coming from unexpected or suspicious sources, especially if linked to high-risk jurisdictions.
- Clients avoiding personal contact or providing limited information during onboarding.
- Abrupt and unexplained shifts in a customer's transaction behaviour or patterns.
- Engaging in activities inconsistent with the business's stated purpose.

4. How do you stay up-to-date with changes in AML and KYC regulations and requirements?

Answer)

For US based banking , we can stay updated on AML KYC norms by :

Government and Regulatory Websites:

FinCEN (Financial Crimes Enforcement Network): The primary US agency responsible for AML and KYC, I regularly access their website for updates, advisories, and rule changes.

Federal Register: Monitor the Federal Register for any new or proposed regulations related to AML and KYC.
Other Relevant Agencies and track relevant information from other agencies like the Department of the Treasury, the Federal Reserve, and state-level financial regulators.

2. Financial Industry Associations and Publications:
American Bankers Association (ABA): Publications and updates from the ABA for their insights on regulatory developments.

Financial Industry Regulatory Authority (FINRA): Relevant FINRA resources for member firms on AML and KYC compliance.

Trade Publications: Monitor leading financial publications like American Banker, Wall Street Journal, and others for news and analysis on regulatory changes.

3. Legal Resources:

Law Firms and Consulting Firms: Reports and articles from legal and consulting firms specializing in financial compliance for their expert perspectives.
Court Decisions: Monitor relevant court decisions that could impact the interpretation or application of AML and KYC regulations.

5. What are the consequences of non-compliance with AML and KYC regulations?

Answer)

Financial Crimes Enforcement Network (FINCEN) plays a key role in enforcing Anti-Money Laundering (AML) and Know Your Customer (KYC) regulations in the US, Penalties and fines are imposed by FINCEN in US Banking, please find the details on the consequences might be faced by Banks

Financial Penalties:

Civil Money Penalties: FINCEN has the authority to impose civil monetary penalties of up to $2.5 million per violation, or twice the amount of funds involved in the violation, whichever is greater. These penalties can quickly escalate, especially for repeated or egregious violations.

Criminal Penalties: Intentional violations of AML/KYC regulations can be prosecuted as criminal offenses, carrying potential fines of up to $5 million and imprisonment for up to 30 years.

Reputational Damage:

Public Enforcement Actions: FINCEN publicly names and shames institutions found in violation of AML/KYC regulations, leading to significant reputational damage and loss of trust from customers, partners, and investors.

Other Consequences:

Exclusion from Government Contracts: Federal agencies may exclude your institution from bidding on government contracts if you are found in violation of AML/KYC regulations.

Professional Sanctions: Regulatory bodies can suspend or revoke professional licenses of individuals involved in non-compliant activities.

Example :

Global Bank AML Fines:

In 2022, global banks faced significant AML fines, with civil monetary penalties exceeding $2 billion. These fines serve as examples of the international impact of AML violations.

BSA-Related Criminal Penalty:

In the USA, a violation of the Bank Secrecy Act (BSA) can lead to a maximum criminal penalty of $250,000 and up to five years' imprisonment.

6. Can you describe the steps involved in conducting a risk assessment for a customer or transaction?

Answer)

Basic Questions on AML

YouTube Channel Link: https://www.youtube.com/@Aml_Transformations

FinCEN provides guidance on conducting a basic BSA/AML risk assessment to determine the level of risk associated with customer accounts, contributing to the overall regulatory framework.

Few steps which are involved in Risk assessment are :

1.Gather Information:

Customer information: Collect and verify detailed information about the customer, including:

1. Full name and aliases
2. Nationality and residency
3. Date of birth and place of birth
4. Address and any known affiliated addresses
5. Business activities and nature of the transaction
6. Beneficial ownership structure
7. Any political affiliations or government positions held

Transaction information:

Obtain specifics about the transaction, such as:

1. Amount of money involved
2. Purpose of the transaction
3. Origin and destination of funds
4. Payment methods used
5. Any intermediary parties involved

2. Screen Against Sanctions Lists:

Resources like the OFAC Specially Designated Nationals and Blocked Persons List (SDN List) and other relevant sanctions lists to compare the gathered information with known sanctioned individuals and entities.

Sophisticated screening tools that can identify potential matches based on phonetic and typographical variations.

3. Risk Analysis & Classification:

Checking the potential for violations: Consider factors like the **customer's location, industry, transaction type, and any red flags** identified during information gathering.

Assign a risk level: Categorize the customer or transaction as low, medium, or high risk based on your analysis.

4. Enhanced Due Diligence (EDD) for High-Risk:

If the risk assessment identifies a high-risk scenario, implement enhanced due diligence measures. This may involve:

1. Gathering additional information about the customer and transaction
2. Verifying the legitimacy of business activities
3. Obtaining independent information sources to corroborate customer details
4. Conducting enhanced screening on additional parties involved

5. Continuous Monitoring:

Monitor ongoing customer activity and transactions for any suspicious behaviour or changes in risk profile. Regularly perform rescreening's against updated sanctions lists.

6. Documentation & Reporting:

Basic Questions on AML

YouTube Channel Link: https://www.youtube.com/@Aml_Transformations

Document all steps taken during the risk assessment process.

Report any potential or actual violations to OFAC as required by regulations.

6.How do you identify politically exposed persons (PEPs) and high-risk customers?

Answer)

Answer to this question depends on lots of parameter in which you need to understand risk , please refer youtube channel for related content.

Tools used for PEP Check :

Complyadvantage , Namescan

Tools used for High Risk Entity/Individual/Geography

OFAC sanctions list, EU Consolidated Sanctions List, UK HM Treasury Consolidated List.

8.Can you explain the difference between transaction monitoring and suspicious activity monitoring?

Answer)

Transaction Monitoring	**Suspicious Activity Monitoring**
Involves the systematic analysis of financial transactions in real-time or historically to detect patterns or behaviours that may indicate illegal activities, such as money laundering or fraud	Continuous scrutiny of customer behaviour and transactions to identify specific activities that appear unusual or suspicious, triggering further investigation.
Often involves real-time analysis of transactions as they occur, aiming to identify anomalies	Analyses patterns and behaviours over a more extended period, aiming to detect trends or consistent suspicious activities that may not be apparent in individual transactions
Detection of irregular patterns or deviations from normal customer behaviour based on transactional data	Targets specific activities that may be indicative of money laundering, fraud, or other illicit financial behaviours
Example : Flagging a large cash deposit by a customer with no history of such transactions.	Example : Investigating repeated money transfers to high-risk jurisdictions or transactions involving known shell companies.

10. Can you describe a time when you had to handle a complex AML or KYC issue?

Answer)

Depends on lot of factors , please refer YouTube channel.