**Financial Crime & Anti-Money Laundering (AML) Policy**

**1. Background**

**1.1 Importance of Financial Crime Controls**

Financial crime, including money laundering, terrorism financing, fraud, and human trafficking, poses significant risks to financial institutions and the global economy. Strong financial crime controls are essential for several reasons:

* **Protecting the Integrity of the Financial System**: Effective AML and financial crime controls help maintain the integrity and stability of the financial system by preventing illicit activities.
* **Reputation Management**: Implementing robust financial crime controls enhances the organization's reputation and fosters trust among customers, investors, and regulators.
* **Preventing Legal and Financial Penalties**: Organizations with inadequate financial crime controls face severe legal and financial consequences, including fines, sanctions, and loss of operating licenses.
* **Corporate Responsibility**: Financial institutions have a moral and ethical responsibility to prevent their services from being used for illegal activities, thus contributing to a safer society.

**1.2 Regulatory Compliance**

Financial institutions are subject to a wide range of local and international regulations designed to combat financial crime. Compliance with these regulations is mandatory and involves:

* **Customer Due Diligence (CDD)**: Verifying the identity of customers and assessing the risk they pose.
* **Transaction Monitoring**: Continuously monitoring transactions for suspicious activities.
* **Reporting Obligations**: Reporting suspicious activities to relevant authorities.
* **Record Keeping**: Maintaining detailed records of transactions and customer information.
* **Employee Training**: Educating employees about AML regulations and red flags.

**1.3 Penalties for Non-Compliance**

Organizations that fail to mitigate financial crime risk and comply with regulatory requirements face various penalties, including:

* **Fines**: Regulatory authorities can impose substantial fines on organizations for non-compliance with AML regulations. These fines can reach millions or even billions of dollars.
* **Sanctions**: Non-compliant organizations may face sanctions, including restrictions on their operations or being barred from certain markets.
* **Reputational Damage**: Public exposure of non-compliance can severely damage an organization's reputation, leading to loss of customers and business opportunities.
* **Operational Impact**: Regulatory actions can disrupt business operations, leading to increased scrutiny and additional compliance costs.
* **Legal Consequences**: Senior management and employees may face personal legal consequences, including criminal charges and imprisonment.

**2. Scope**

This policy applies to all business units within Barclays and its subsidiaries. It is designed to ensure that the organization complies with all local and international AML regulations and guidelines.

**3. Definitions**

* **Money Laundering**: The process of concealing the origins of money obtained illegally, typically by means of transfers involving foreign banks or legitimate businesses.
* **Terrorism Financing**: The provision of funds or financial support to terrorist organizations or individual terrorists.
* **Sanctions**: Restrictions imposed by governments or international bodies on certain countries, entities, or individuals to achieve foreign policy and national security objectives.
* **Customer Risk**: The potential risk posed by customers based on their profile, nature of business, geographic location, and transaction patterns.
* **Product Risk**: The potential risk associated with the financial products offered, considering their complexity, value, and susceptibility to misuse for money laundering or terrorism financing.
* **Transaction Monitoring**: The process of reviewing, analyzing, and monitoring customer transactions to detect and report suspicious activities.
* **Fraud**: Wrongful or criminal deception intended to result in financial or personal gain. Examples include identity theft, account takeover, insider fraud, and location fraud.
* **Know Your Customer (KYC)**: The process of verifying the identity of the organization's clients, assessing potential risks of illegal intentions for the business relationship, and ensuring compliance with AML regulations.
* **Human Trafficking**: The illegal trade of humans for the purposes of forced labor, sexual slavery, or commercial sexual exploitation.
* **Country/Geographic Risk**: The potential risk posed by customers or transactions involving countries with high levels of corruption, weak AML regulations, or active conflict zones.
* **Adverse Media**: Negative information available in the public domain about an individual or organization, indicating potential involvement in illegal activities.

**4. Customer Risk**

**4.1 Risk Assessment**

* **Low Risk**: Customers with transparent and verifiable sources of income, e.g., salaried employees.
* **Medium Risk**: Small business owners with moderate transaction volumes.
* **High Risk**: Politically Exposed Persons (PEPs), customers from high-risk countries, and those with complex business structures.

**4.2 Risk Mitigation**

* Enhanced due diligence for high-risk customers.
* Regular review and update of customer information.
* Continuous monitoring of transactions for unusual activities.

**4.3 Scenarios**

* **Low Risk**: A salaried employee from a reputable company with a straightforward salary deposit pattern.
* **Medium Risk**: An owner of a small retail business with moderate, consistent cash deposits.
* **High Risk**: A customer from a high-risk country who frequently changes the ownership structure of their business.
* **High Risk**: A Politically Exposed Person (PEP) with complex financial dealings and multiple offshore accounts.
* **Medium Risk**: A freelancer with fluctuating income patterns from various international clients.
* **Low Risk**: A retired individual receiving a regular pension payment with minimal other transactions.
* **High Risk**: A customer using multiple accounts to conduct transactions in high-risk jurisdictions without clear economic rationale.
* **High Risk**: A customer with a complex corporate structure involving multiple shell companies.

**5. Product Risk**

**5.1 Risk Assessment**

* **Low Risk**: Standard savings accounts, low-value insurance products.
* **Medium Risk**: Investment products, foreign currency accounts.
* **High Risk**: Private banking, high-value insurance products, and prepaid cards.

**5.2 Risk Mitigation**

* Restricting high-risk products to low-risk customers.
* Implementing transaction limits and enhanced monitoring for high-risk products.

**5.3 Scenarios**

* **Low Risk**: A customer holding a standard savings account with predictable transaction patterns.
* **Medium Risk**: A customer investing in moderate-risk mutual funds with regular contributions.
* **High Risk**: A private banking client with substantial international wire transfers and investments in high-value insurance products.
* **High Risk**: A customer purchasing high-value insurance products with a lump-sum payment from an unknown source.
* **Medium Risk**: A customer maintaining a foreign currency account with frequent transactions in volatile currencies.
* **Low Risk**: A customer using a low-value prepaid card for everyday purchases.
* **High Risk**: A customer frequently purchasing and redeeming gift cards in large quantities.
* **Medium Risk**: A customer using an investment product with moderate risk for speculative trading activities.
* **High Risk**: A customer purchasing precious metals and storing them in offshore locations.

**6. Transaction Monitoring Risk**

**6.1 Risk Assessment**

* Regular transactions vs. irregular, high-value transactions.
* Transactions involving high-risk jurisdictions.

**6.2 Risk Mitigation**

* Implementing automated transaction monitoring systems.
* Setting up alerts for unusual transaction patterns.
* Regularly updating monitoring rules based on emerging risks.

**6.3 Scenarios**

* **Regular Transactions**: Monthly salary credits and utility bill payments.
* **Irregular High-Value Transactions**: Sudden, large transfers to multiple international accounts.
* **High-Risk Jurisdictions**: Frequent transactions to and from countries known for lax AML regulations.
* **Structuring**: Multiple smaller transactions below reporting thresholds that aggregate to a large sum.
* **Flow Through of Funds**: Rapid movement of funds through multiple accounts with no apparent business rationale.
* **Excessive Cash Deposits**: Large cash deposits inconsistent with the customer’s known business activities.
* **Transfers to Suspicious Countries**: Frequent transfers to countries with high levels of corruption or weak AML controls.

**7. Fraud Risk**

**7.1 Risk Assessment**

* Internal and external fraud risks.
* Fraudulent transactions involving stolen identities or compromised accounts.

**7.2 Risk Mitigation**

* Implementing robust internal controls.
* Regular audits and employee training.
* Deploying advanced fraud detection systems.

**7.3 Fraud Scenarios**

* **Identity Theft**: Unauthorized use of someone else’s personal information to open accounts or conduct transactions.
* **Account Takeover**: Unauthorized access to a legitimate customer's account to conduct fraudulent activities.
* **Insider Fraud**: Employees abusing their access to commit fraud.
* **Synthetic Identity Fraud**: Creating a fictitious identity using a combination of real and fabricated information to commit fraud.
* **Phishing**: Deceptive attempts to obtain sensitive information by masquerading as a trustworthy entity in electronic communications.
* **Card-Not-Present Fraud**: Unauthorized transactions made without the physical presence of the card.
* **Location Fraud**: Transactions conducted from locations inconsistent with the customer's usual activity or declared residence.

**8. KYC Risk**

**8.1 Risk Assessment**

* Incomplete or outdated customer information.
* Customers unwilling to provide necessary documentation.

**8.2 Risk Mitigation**

* Comprehensive KYC procedures at the time of account opening.
* Periodic review and updating of customer information.
* Enhanced due diligence for high-risk customers.

**8.3 Scenarios**

* **Incomplete Information**: A customer fails to provide full identification details during account opening.
* **Outdated Information**: A long-time customer has not updated their contact or business information for several years.
* **Unwilling Customer**: A customer refuses to provide additional documentation requested for due diligence purposes.
* **False Information**: A customer provides falsified or misleading information during the KYC process.
* **Complex Ownership Structure**: A corporate customer with an overly complex ownership structure that obscures the identity of beneficial owners.

**9. Human Trafficking Risk**

**9.1 Risk Assessment**

* Transactions indicative of human trafficking activities.
* Customers involved in industries with a high risk of human trafficking.

**9.2 Risk Mitigation**

* Training employees to recognize red flags.
* Collaborating with law enforcement agencies.
* Implementing specific monitoring rules for high-risk industries.

**9.3 Scenarios**

* **Multiple Small Transfers**: Numerous small transactions from various locations that may indicate payment for trafficked individuals.
* **Unusual Business Activity**: A business with high cash flow but no apparent legitimate business activity or inconsistent business narrative.
* **Red Flag Indicators**: Transactions that include keywords associated with human trafficking or sudden changes in transaction patterns.
* **High-Risk Industry**: Transactions involving businesses in industries known for high human trafficking risk, such as certain manufacturing sectors.
* **Unusual Payment Methods**: Use of prepaid cards or virtual currencies in a pattern that suggests avoidance of detection.
* **Suspicious Account Activity**: Frequent deposits and withdrawals with no clear economic purpose, especially involving third parties.
* **Inconsistent Personal Information**: Discrepancies in customer details that suggest identity misuse or concealment.
* **Unusual Travel Patterns**: Travel-related expenses inconsistent with the customer’s known profile or business activities.
* **Third-Party Payments**: Transactions where payments are made by third parties with no apparent connection to the customer.

**10. Country/Geographic Risk**

**10.1 Risk Assessment**

* Customers and transactions involving high-risk jurisdictions.
* Products and services offered in high-risk countries.

**10.2 Risk Mitigation**

* Enhanced due diligence for customers from high-risk jurisdictions.
* Restricting or prohibiting transactions with certain high-risk countries.
* Regular review of country risk ratings.

**10.3 Scenarios**

* **High-Risk Jurisdiction**: A customer from a country with high levels of corruption and weak AML regulations.
* **Sanctioned Country**: Transactions with a country under international sanctions.
* **Geographic Concentration**: A high volume of transactions from a specific high-risk region.

**11. Sanctions Risk**

**11.1 Risk Assessment**

* Transactions involving sanctioned countries, entities, or individuals.
* Products and services offered to high-risk customers.

**11.2 Risk Mitigation**

* Screening customers and transactions against sanctions lists.
* Implementing automated sanctions screening systems.
* Training employees on sanctions compliance.

**11.3 Scenarios**

* **Sanctioned Entity**: A transaction involving an entity listed on the OFAC sanctions list.
* **Appearing on an OFAC List**: A customer or counterparty is identified on the Office of Foreign Assets Control (OFAC) Specially Designated Nationals (SDN) list.
* **Dual-Use Goods**: A customer attempting to export goods that can be used for both civilian and military purposes to a sanctioned country.
* **False Documentation**: A customer providing falsified documents to disguise dealings with a sanctioned entity.

**12. Terrorism Financing Risk**

**12.1 Risk Assessment**

* Customers and transactions with potential links to terrorist activities.
* Products and services susceptible to misuse for terrorism financing.

**12.2 Risk Mitigation**

* Enhanced due diligence for high-risk customers.
* Implementing transaction monitoring rules specific to terrorism financing.
* Collaborating with law enforcement agencies.

**12.3 Scenarios**

* **Charitable Donations**: Large donations to charities with links to terrorist organizations.
* **Cash Intensive Businesses**: Businesses with high cash turnover that may be used to finance terrorism.
* **Unusual Transactions**: Transactions that have no clear economic purpose and may indicate support for terrorist activities.

**13. Adverse Media Screening and Third-Party Platforms**

**13.1 Adverse Media Screening**

* Regular screening of customers and transactions against adverse media reports using specialized platforms.

**13.2 Platforms**

* **World-Check**: Screening customers against global risk intelligence data, including PEPs, sanctions, and adverse media.
* **Companies House**: Verifying the legitimacy and structure of corporate customers.
* **Image Detection**: Using image recognition technology to verify customer identities and detect fraudulent documents.
* **Other Platforms**: Utilizing additional sources such as LexisNexis, Dow Jones Risk & Compliance, and Google Alerts for comprehensive due diligence.

**13.3 Scenarios**

* **Adverse Media Match**: A customer is identified in adverse media reports related to financial crimes.
* **PEP Detection**: World-Check identifies a new customer as a politically exposed person (PEP).
* **Corporate Structure Verification**: Companies House data reveals discrepancies in a corporate customer's declared business structure.
* **Fake Document Detection**: Image recognition technology detects anomalies in submitted identification documents.