**Red Flags for Money Laundering:**

Criminals have developed sophisticated ways to conceal the origin of illegally earned money.  Due to the evolving nature of money laundering tactics, organizations end up investing a lot of time, labor, and financial resources to combat Money Laundering

**What are AML Red Flags?**

Money Laundering is a serious crime that can lead to a variety of financial and legal consequences for financial institutions, governments, and other businesses that handle large sums of money. It is essential to be aware of the 12 red-flag indicators that point to illegal activities so you can protect your business from financial crimes and penalties from Anti-Money Laundering Regulators..

**1. Frequent Cross-Border Money Transfers to Different Accounts**

This red flag can include:

- Rapid transfers that are sent in large, round dollar, hundred dollar or thousand dollar amounts.

-Significant incoming funds transfers received on behalf of a foreign client with little or no explicit reason.

- Payments or receipts with no apparent links to legitimate contracts, goods or services received.

- By moving money between accounts in different countries, criminals are able to conceal the origin of the funds in an effort to avoid detection from authorities.

**2. Unusual Transaction Patterns (UTPs)**

Firms should look out for large or multiple transactions that don’t follow a customer’s typical behavior. Sudden increases in customer activity and transactions with no apparent economic purpose can suggest criminal activity.

**3. Complex Ownership Structure or Use of Shell Companies**

[Shell companies](https://www.sigma360.com/knowledge-center/shell-companies) are used to hide the identity of true owners behind nominees and trusts. While there are legitimate reasons to set up shell companies, money launderers will take advantage of the lack of ownership transparency in order to conceal the flow of illegal funds. Shell companies can be used to purchase assets, open bank accounts, and carry out transactions that are difficult to trace back to the true source, and that’s why they’re a red flag to watch out for.

**4. Ultimate Beneficial Owner (UBO) Concerns**

It is important to identify the persons who ultimately own or control a customer and/or on whose behalf a transaction is being conducted. Any discrepancies or inconsistencies in [UBO information](https://www.sigma360.com/knowledge-center/ultimate-beneficial-owner) can serve as a red flag for potential money laundering or terrorist financing activities.

**5. Individuals with High Positions**

Typically relates to [Politically Exposed Persons (PEPs)](https://www.sigma360.com/knowledge-center/politically-exposed-persons), such as foreign government officials (heads of state, legislators, judicial or military officials), officials in political parties, or other more senior appointed officials. Through their public positions, these individuals may be more vulnerable to corruption and could pose a higher risk of money laundering.

**6. Appear on Relevant Sanctions Lists**

Firms should review relevant international sanctions lists to ensure that customers are not sanctioned themselves or transacting with a sanctioned entity. Criminals are finding new ways, both high and low-tech, to evade institutional controls set up to prevent the movement of funds by sanctioned individuals/entities. Firms need to have a real-time plan for managing rapid changes to sanctions lists.

**7. Associated with Adverse Media**

Adverse media screening is the process of examining third-party data sources for negative news about an individual or company. These reviews are critical to discovering a client’s involvement in activities related to financial crime or ones that pose a reputational risk. Teams that use [manual Google searches](https://www.sigma360.com/knowledge-center/does-using-google-search-strings-for-adverse-media-screening-work) for adverse media are switching to technology that is less costly and more effective when tackling this red flag.

**8. Account Profile Inconsistencies**

This can include false identification documentation to conduct transactions and variations in the spelling of names, addresses and value of funds transfers that are inconsistent with a customer’s profile.

**9. CDD Irregularities**

Customer Due Diligence is a series of checks done to verify identities and assess risk as part of KYC. Any customers flagged during CDD for higher money laundering or terrorist financing risks present increased risk exposure to a bank and require [Enhanced Due Diligence steps](https://www.sigma360.com/knowledge-center/what-is-enhanced-due-diligence) to ensure it’s safe to onboard them.

**10. Suspicious Employee Activity**

Employee activity can also signal an AML red flag, for example if an employee lives a lavish lifestyle that cannot be supported by their salary or an employee is reluctant to take a vacation.

### 11. Purchasing of Precious Metals

Money launderers value precious metals in their trade because of their high intrinsic value, convertibility, and potential for anonymity in transfers. Buying expensive jewelry or bullion bars with cash and then selling at a profit doesn’t require documenting the transaction or declaring the profits and can be used as a tactic for money laundering.

### 12. High-Risk Countries

Publicly identified jurisdictions with significant strategic deficiencies in their AML/CFT/CPF is cause for concern because criminals can exploit [countries with weak or absent national measures for AML](https://www.sigma360.com/solutions/risk-ratings) laws and regulations.