Suspicious Activities List

The following is a list of suspicious activities segmented in terms of type of financial institution. Keep in mind that the activities listed here are not exhaustive and definitive. Sophisticated money launderers are well aware of suspicious activities lists and are continuously inventing new techniques that do not involve the activities listed here.

THIS LIST IS A GENERAL LIST OF SUSPICIOUS ACTIVITIES. ALSO MAKE SURE YOU FAMILIARISE YOURSELF WITH (A) ANY LIST PROVIDED BY THE FINANCIAL REGULATOR IN YOUR COUNTRY AND (B) YOUR INSTITUTION’S SUSPICIOUS ACTIVITIES LIST.

---

**Commercial Banking**

1. Accounts are used to receive or disburse large sums but show virtually no normal business-related activities, such as the payment of payrolls, invoices, etc.

2. Customer seems unconcerned with terms of credit or costs associated with completion of a loan transaction.

3. Back-to-back deposits/loans without any identifiable and legally-admissible purpose. Especially, if with subsidiaries of, or affiliates of, overseas financial institutions in known drug trafficking areas.

4. Customer makes a large volume of cash deposits from a business that is not normally cash-intensive.

5. Unexplained transactions are repeated between personal and commercial accounts.

6. Provision of bank guarantees or indemnities as collateral for loans between third parties that are not in conformity with market conditions. In general, use of guarantees as collateral needs to be watch particularly if they are from a bank located in another country.

7. Provision of collateral by way of pledge or guarantee without any discernible plausible reason by third parties unknown to the bank and who have no identifiable close relationship with the customer. Lack of credit information on third party obligor.

8. A request for loans to an offshore company, especially one located in a financial haven country, or for a loan secured by obligations of an offshore bank.

9. Customer collateralizes loan with cash deposit; or customer uses cash collateral located offshore to obtain loan.

10. Proceeds of loan are used for a purpose other than the purpose recorded.
11. For Corporate and Trade Finance customers, particular emphasis should be paid in the credit review stage. In addition, such customers should be watched carefully for a change in management owing to an acquisition or, even if management is retained, watch for a change in ownership. This should also be done for non-facility customers. Wherever there is a change in ownership, the account must be placed under enhanced scrutiny to ensure that there is no significant change in patterns of transactions (e.g., a cash-intensive business suddenly has a doubling of cash deposited on account of supposedly enhanced business, which appears unrealistic).

12. Customers who repay classified/problem loans before the expected time and for larger amounts than anticipated, with no reasonable explanation of the source of funds.

13. Customers who make regular and large payments using different means, including electronic payments that cannot be clearly identified as bonafide transactions, make to or receive regular and large payments from countries which are identified as large drug markets or known for highly secretive banking and corporate law practices and or with no apparent business connection.

14. Customer consistently makes immediate large withdrawals from an account that has just received a large and unexpected credit from abroad by EFT.

15. Trade pricing is not one that one expects for the goods being exported or imported.

16. Customer claiming to be an importer seems to lack basic knowledge of letter of credit. Claims to be doing a small test import from a new supplier followed by a large import.

17. Presentation of huge value international bill of exchange for discounting at bank on open account i.e. without LC. This can be sale bill discounting (initiated by exporter, pay to exporter) or purchase bill discounting (at request of importer, pay to exporter). Normally the risk lies in sale bill discounting, which an exporter may initiate with forged documentation proving satisfactory movement of goods and receipt in good condition/bogus underlying export of goods, although some goods may have been sent. Purchase bill discounting is usually extended to well-established corporations for procuring raw materials and is less risky. LC backed bill discounting is usually relatively risk free if the importer bank establishing the LC / the corporate setting up the LC, are reputed.

However, in most cases related to bills of exchange (other than where the parties are clearly very reputed), the underlying trade pricing needs to be looked at, because this may be the variable being used to launder money.

18. Use of letters of credit and other methods of trade finance to move money between countries, where such trade is not consistent with the customer’s usual business. In this connection, banks should strictly adhere to the following:

1. To exercise prudence in cases where the beneficiaries of the letters of credit or the shipping companies, are owned by the bank customer, who opens these letters.
2. Amounts on letters of credit submitted by the customer to the bank and to the Customs/Port/ Airport authorities should match the original.
3. Checking of documents should be on selective and regular basis with the shipping companies and Customs/Port/ Airport authorities.
4. Also, the size of the facilities should be in line with the securities on hand, nature of business and net worth of the customer.

Commercial Banking – Tax evasion

There will be circumstances where a bank suspects that there is tax evasion being undertaken by a customer involved in an otherwise legitimate business or occupational activity. *These transactions might typically be noticed when the bank or other institution reviews their customer's business.* Employees of banks and other institutions are expected to know their customers' financial and business affairs to the point where they are able to serve the duties of the bank or other financial institution. Suspicions may arise when they review the accounts following the submission by the customer of the annual profit and loss and balance sheet. Similarly, suspicions may arise at other points, such as when a new loan is applied for by the customer. Financial institutions should report suspect tax evasion transactions encountered in their dealings with corporate customers as well as other customers. While this reporting responsibility may not be explicitly laid out in the anti-money laundering regulations, it may be implied by the applicable income tax laws.

International profit shifting or funds transfer to avoid local taxation or to launder money.

There may be instances of international profit shifting or funds manipulation that may result in suspicious transactions involving tax evasion or money laundering - this could involve schemes whereby residents use incentive tax rates (for non resident customers) to evade a resident's income tax obligations. For example this may involve opening or operating an account in the name of a non resident where the account is in fact exclusively or predominantly used by a resident. Suspicious circumstances include:

1. Change of address of an existing account holder to an overseas address where the account continues to be operated predominantly within the country.
2. Payment of management fees to related companies in a way that appears designed to transfer profit offshore to evade tax.
3. Changes of ownership of a foreign company in a corporate group, 'balance day adjustments' and other actions at year end which appear designed to shift profit offshore to evade the countries tax obligations.

Use of cheques for tax evasion

There are many ways in which cheques are used in the evasion or attempted evasion of tax. Some examples:
1. Situations where a customer operates an account to which the deposits are predominantly third party cheques.

2. Situations where cheques made out to a business name are not put through the normal trading account of the business but are either deposited into another account (this account could be in the name of director/partner or family member of the director/partner) or cashed over the counter.

3. Situations where a trading account customer cashes a cheque (drawn on the trading account) over the counter although the cheque is made out to a third party.

**Commercial Banking – Terrorist Financing**

Money laundering linked to terrorist activities will typically involve instances in which simple operations have been performed (retail foreign exchange operations, international transfer of funds) revealing links with other countries. Some of the customers may have police records, particularly for trafficking in narcotics and weapons, and may be linked with foreign terrorist groups.

The following patterns of activity indicate collection and movement of funds that could be associated with terrorist financing:

1. Use of multiple personal and business accounts to collect and funnel funds to a small number of foreign beneficiaries
2. Deposits are followed within a short period of time by wire transfers of funds
3. Beneficiaries are located in a problematic foreign jurisdiction
4. Structuring of cash deposits in small amounts in an apparent attempt to circumvent local/ internal currency transaction reporting requirements
5. Mixing of cash deposits and monetary instruments
6. Deposits of a combination of monetary instruments atypical of legitimate business activity (business checks, payroll checks)
7. Stated occupations of those engaging in transactions that are not commensurate with the level of activity (e.g., student, unemployed, self-employed)
8. Large currency withdrawals from a business account not normally associated with cash transactions
9. Movement of funds through a FATF “non-cooperative country or territory”
10. Involvement of multiple individuals from the same country or community

In general, *not for profit organizations*, especially those with a religious or political purpose, professed social service organizations with a religious link etc., need to be watched carefully, as it has been found that terrorist organizations receive funding from these legitimate organizations through their collections – donations, subscriptions etc. Terrorists have also been found to use debit cards issued by offshore banks.

---

**Merchant Banking**
The following examples highlight circumstances in which a merchant bank or similar financial institution may become an unwitting participant in a money laundering transaction.

1. A corporate customer facing liquidation has US$300m in non-performing loans with your bank. You are informed by a director that the debt will be cleared from a facility recently arranged with a European merchant bank. You can find no reference to the merchant bank in any of the banking almanacs and consider that no-one would lend commercially in these circumstances. You suspect that the source of the funds may be the proceeds of crime.

2. Press reports of the arrest of an international drug syndicate lead you to consider whether your firm inadvertently may have been involved in laundering the proceeds of the syndicate's criminal activities. On reviewing the relevant customer files you come to the view that information available to you at the time should have put you on notice that the funds which passed through a number of the accounts may have been tainted. You subsequently obtain legal advice that the partners of the firm may be vulnerable to a money laundering charge and that, to protect them, you should immediately lodge a suspect transaction report.

3. You arrange a loan of US$2,000,000 at 4% p.a. for a customer who wishes to expand a business operation. The monthly interest is paid by cheque regularly for three months. You then notice that, over the next three month period, the interest is paid by three or more cash payments each month and never by cheque as before. The cash payments are roughly equal in amount and are all under US$10,000. You suspect that the customer is trying to evade the requirement that cash transactions of US$10,000 and over be reported to the country FIU.

4. As the underwriter of a share issue you learn that an employee of your firm has placed a parcel of shares with a customer who paid with US$100,000 in cash. The customer is a businessman who runs a chain of fast-food outlets. You know that another person involved in running the same business has recently been charged with importing prohibited drugs. You suspect that the cash payment for the shares is connected with tax evasion and/or laundering funds received from the drug trafficking.

5. You are an executive director of a merchant bank that has recently taken over another merchant bank. You discover that, late in June, the newly acquired bank advanced a temporary loan of US$10 million to a company for the purpose, it seems, of deceiving shareholders and creditors as to the state of the company's liquidity. The loan was repaid a week later. You suspect that the parties involved in the transaction committed the offence of money laundering and that the money repaid under the loan was tainted by that crime.

6. Your merchant bank is asked by a customer to review, and where necessary, to recommend changes in its corporate financial structure. During the course of the review you discover that the company has an extensive network of subsidiary companies and that some of these companies have been used for the purpose of fraudulently misrepresenting the amount of income tax payable. Apart from the possibility of tax evasion offences, you suspect that the offence of money-
laundering has been committed on numerous occasions when tainted funds have been transferred from company to company with the group.

**Merchant Banking - Tax Evasion**

The following examples highlight circumstances in which a merchant bank or similar financial institution may become an unwitting participant in a tax evasion transaction.

1. An resident public company has an offshore bank account with a branch of your merchant bank in a tax haven country. You receive instructions from the company to expect substantial deposits into the offshore account from a third party. You later discover that the third party is a European wholesaler and that the deposits are part payment for exports made by the resident company. You suspect that the arrangement is designed to evade income tax.

2. A corporation seeks to roll over a bill facility and in support provides financial statements for the last tax year. The level of security is assessed as being marginal and the managing director provides additional information that cost of work in progress at balance date was understated in the books as it did not take into account accumulated overheads. The managing director intimated that full accounting for overhead costs would be made at the time of completion of the relevant contracts. You suspect an unlawful tax deferral scheme.

3. As the underwriter of a share issue you learn that an employee of your firm has placed a parcel of shares with a customer who paid with US$100,000 in cash. The customer is a businessman who runs a chain of fast-food outlets. You know that another person involved in running the same business has recently been charged with importing prohibited drugs. You suspect that the cash payment for the shares is connected with tax evasion and/or laundering funds received from the drug trafficking.

4. Your merchant bank is asked by a customer to review, and where necessary, to recommend changes in its corporate financial structure. During the course of the review you discover that the company has an extensive network of subsidiary companies and that some of these companies have been used for the purpose of fraudulently misrepresenting the amount of income tax payable. Apart from the possibility of tax evasion offences, you suspect that the offence of money-laundering has been committed on numerous occasions when tainted funds have been transferred from company to company with the group.

**Private Banking/ Broker-Dealers/ Investment Management Companies**

1. Customer exhibits unusual concern regarding the firm's compliance with government reporting requirements, particularly with respect to the customer's identity and type of business assets.

2. Customer is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspect identification or business documents.
3. The customer wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the customer’s stated business strategy.

2. Customer is associated with a person that is the subject of news reports indicating possible criminal, civil, or regulatory violations.

3. Customer appears to be acting as an agent for another entity but declines, or is reluctant, without legitimate commercial reasons, to provide any information in response to questions about such entity.

4. Customer has difficulty describing the nature of his or her business or lacks general knowledge of the industry in which he or she purportedly is engaged.

5. The customer exhibits a lack of concern regarding risks, commissions, or other transaction costs.

6. For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.

7. The customer’s account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.

8. The customer’s account has a large number of wire transfers to unrelated third parties inconsistent with the customer’s legitimate business purpose.

9. The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.

10. The customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account.

11. Buying and selling of a security with no discernible purpose in circumstances which appear unusual, e.g. churning at the customer’s requests.

12. The entry of matching buys and sells in particular securities ("wash trading"), thereby creating an illusion of trading. Such wash trading does not result in a bona fide market position, and might provide "cover" for a money launderer.

13. Wash trading though multiple accounts might be used to transfer funds between accounts by generating offsetting losses and profits in different accounts. Transfers of positions between accounts that do not appear to be commonly controlled also could be a warning sign.

14. Abnormal settlement instructions including payment to apparently unconnected parties.

15. Transactions not in keeping with normal practice in the market in which they relate, e.g. with reference to market size and frequency, or at off market prices,
early termination of products at a loss due to front end loading, or early
cancellation, especially where cash had been tendered and/or the refund cheque
is to a third party.

16. The customer, for no apparent reason or in conjunction with other “red flags,”
engages in transactions involving certain types of securities, such as penny
stocks, Regulation “S” (Reg S) stocks, and bearer bonds, which although
legitimate, have been used in connection with fraudulent schemes and money
laundering activity. (Such transactions may warrant further due diligence to
ensure the legitimacy of the customer’s activity.)

17. A large number of security transactions across a number of jurisdictions.

18. Customer engages in multiple transfers of funds or wire transfers to and from
countries that are considered bank secrecy or "tax havens" that have no apparent
business purpose or transfers funds to or from countries listed as non-cooperative
by FATF, or are otherwise considered by the firm to be high-risk

19. Settlement either by registration or delivery of securities to be made to an
unverified third party.

20. Customers who wish to maintain a number of trustee or customers’ accounts that
do not appear consistent with their type of business, including transactions which
include nominee names.

**Tax evasion example**

A money market account with a substantial credit balance is in the name of a non-
resident. Interest is accumulated in the account, after deducting withholding tax (if
any). You receive information that the beneficial owner of the funds is a resident and
suspect that the account may be a vehicle to evade tax.

---

**Life Insurance Companies**

Money laundering risk should not be predicated solely on the existence of an ability to
obtain a refund on a purchased financial product. Rather, the focus should be on the
ability of a money launderer to use a particular financial product to store and move
illicit funds through the financial system. Therefore insurance products with
investment features, and insurance products possessing the ability to store value and
to transfer that value to another person, are important. Life insurance products
appear to have been particularly attractive to narcotics money launderers.

1. Transactions where the nature, size or frequency appears unusual, for example,
customer requests for early termination or cancellation (within one year from date
of inception) of a single premium policy, especially where cash had been
tendered.

2. Unusual transaction (e.g., a person residing in another city with little connection
to the city in which you have your branch, requests a life insurance policy).
3. Transactions that are incompatible with the customer's normal activity or are beyond the customer's apparent financial means (e.g., the customer requests a single premium contract with a large sum-assured).

4. Transactions in which funds are received by way of a third party cheque, especially where there is no apparent connection between the third party and the customer.

5. Abnormal settlement instructions, including payment to apparently unconnected parties or to countries in which the insured is not known to operate.

6. A sudden request for a significant purchase of a lump sum contract from an existing customer whose current contracts are small and of regular payment only.

7. A life insurer receives large or unusual premium payment in cash from customer. In particular, a life insurer should be vigilant in verifying information and the nature of transaction of any customer if any single payment is in cash exceeding US$10,000.

8. Transactions in which funds are received from or paid to a customer's account in a financial haven country, or in foreign currency especially when such transactions are not consistent with the customer's transaction history.

9. Overpayment of premium with a request to refund the excess to a third party or to a different country.

10. Assignment of a policy to unidentified third parties and for which no plausible reasons could be ascertained.

11. A number of policies taken out by the same insured for low premiums, each purchased for cash and then cancelled with return of premium to a third party.

12. A policyholder may exercise cancellation rights or cooling off rights on life insurance products where the sum invested must be repaid (subject to any shortfall deduction where applicable). This could offer a readily available route for laundering money, and life insurers and their agents should therefore be alert to any abnormal exercise of cancellation /cooling off rights by any policyholder. In the event that abnormal exercise of these rights becomes apparent, the matter should be treated as suspicious and reported through the usual channels.

13. Employees or agents who have consistently high activity levels of single premium business far in excess of any average company expectation.

14. The use of an address that is not the customer's permanent address (e.g., utilization of the agent's office or home address for the dispatch of customer documentation).

Life insurance policies can similarly be used in terrorist financing.