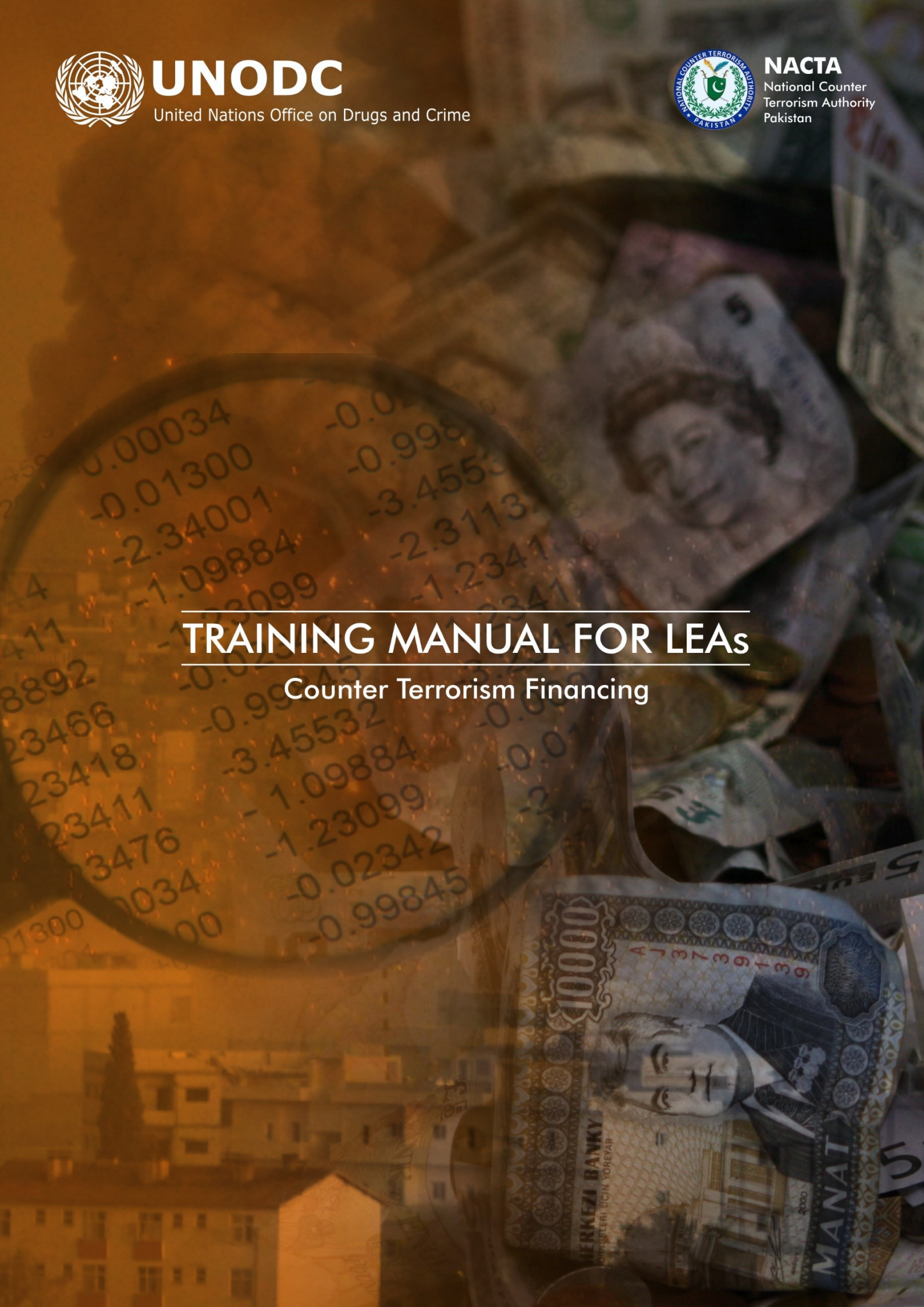
UNODC
United Nations Office on Drugs and Crime

NACTA
National Counter Terrorism Authority
Pakistan



TRAINING MANUAL FOR LEAs

Counter Terrorism Financing

Acronyms and Abbreviations

Table of Content

Terrorist Finance and Money Laundering Investigation Training Manual

This manual covers International and national relevant legal regime with respect to offence of terror financing and money laundering. It also caters for the need to understand TF/AML and its sources, in the context of Pakistan. Moreover, all stages of terrorist finance and money laundering investigation have been incorporated with examples and typologies for the investigators to better understand how to conduct proactive and parallel financial investigations and identify cases that they come into contact with. It seeks to provide methods and techniques relevant to Pakistani legislation as well as successful international practices. It consists of the following main sections:

1. International Context
2. Pakistani Legislation
3. Understanding Terrorist Finance and Money Laundering
4. Sources of TF
5. Powers of Financial Investigators
6. Gathering Evidence and Conducting Financial Investigations

    6.1 - Sources of Intelligence

    6.2 - Developing a Financial investigation Strategy

    6.3 – Identifying Potential Targets/ Tactics

    6.4 – Surveillance

    6.5 – Searches

    6.6 – Undercover Operations

    6.7 – Financial Profiles

    6.7 -Company Profiles

    6.8 – Interviews

    6.9 - Forensic Accountants

    6.10 - Inter-Agency Co-operation/Joint Investigation Teams

    6.11 - Phases of Financial Investigation

        - Open, plan and register
        - Conduct Investigation
        - Judicial Phase
        - Confiscation Phase

7. Foreign Assistance in Financial Investigation

    - Mutual legal assistance
    - Confiscation
    - Asset Recovery
    - Extradition

8. Training Methodology

- Practical exercises
- Lectures
- Workshops

Section 1 - The International Context

What is Terrorism?

There is no universal definition of terrorism as many states have different views as to what it should contain.

The International Convention for the Suppression of the Financing of Terrorism 1999 described the primary objective of terrorism is 'to intimidate a population, or to compel a government or an international organisation to do or abstain from doing any act.'

The United Nations General Assembly in 1994 condemned terrorist acts and used the following definition. 'Criminal acts intended or calculated to provoke a state of terror in the general public, or a group of persons or particular persons for political purposes are in any circumstances unjustifiable whatever the considerations of a political, ideological, racial, ethnic, religious or any other nature that may be involved to justify them.'

The Pakistan Anti-Terrorist Act 1997 further defines offences of terrorist finance as; 'a person commits an offence if he uses money or other property for the purposes of terrorism, or possesses money or other property; and intends that it should be used or has reasonable cause to suspect it may be used for the purposes of terrorism.'

'Combating the financing of terrorism is an inescapable obligation of all states' (World Bank).

1.1 The United Nations Sanctions Regime have attempted to focus attention on specific issues through the issuing of United Nations Security Council Resolutions (UNSCRs).

UNSCR 1267 established a sanctions regime to cover individuals associated with Al Qaida, Osama Bin Laden and the Taliban.

Imposes the following sanctions:

Assets Freeze

- All states are required to **freeze without delay** the funds and other financial assets or economic resources of designated individuals and entities.

Travel Ban

- All states are required to **prevent the entry** into or transit through their territories by designated individuals

Arms Embargo

- All states are required to prevent the **direct or indirect supply, sale and transfer from their territories** or by their nationals outside their territories or using their flag vessels or aircraft, of **arms and related material of all types**, spare parts, and technical advice, assistance, or training related to military activities, to designated individuals and entities.

UNSCR 1373 underlined the necessity for states to have legislation to establish terrorist acts as serious criminal offences and provide the mechanisms for the freezing and seizure of the assets of terrorists and proscribed organisations.

- Adopted by the security Council on 28th September 2001

- UN member states to adjust national laws to ratify existing International Conventions on Terrorism
- All States to ensure that terrorist acts are established as serious criminal offences in domestic laws and regulations and that the seriousness of such acts is duly reflected in sentences served.

Requires member states to:

- **Prevent and Supress** the financing of terrorist acts
- **Criminalise** the wilful provision or collection of funds by their nationals or in their territories to carry out terrorist acts
- **Freeze without delay** funds or other financial assets or economic resources of persons who commit or attempt to commit terrorist acts or participate in or facilitate the commission of terrorist acts
- **Prohibit** their nationals or any persons and entities within their territories from making any funds, financial assets or economic resources or financial or other related services available, directly or indirectly, for the benefit of persons who commit or attempt to commit commission of terrorist acts.

The difference between UNSCR 1267 and 1373 is that the former designated Al Qaeda, the Taliban and Osama Bin Laden to be targeted by the sanctions, whereas the latter requests that the state (Pakistan) develops its own legislation to proscribe terrorist organisations and individuals

1.2 The Financial Action Task Force (FATF) is an intergovernmental body whose purpose is to establish and develop and promote policies, both at national and international levels to combat money laundering and the financing of terrorism. FATF and FATF-Style Regional Bodies will work together with international organisations to develop proposals to strengthen all counter-terrorism financing tools and to ensure that they are working effectively. FATF provide a list of 40 +9 Recommendations to assist states in their fight against terrorism.

R.5 - Criminalizing Terrorist Financing

- Countries should criminalize terrorist financing on the basis of the Terrorist Financing Convention
- Criminalize the financing of terrorist acts
- Criminalize the financing of terrorist organisations and individual terrorists even in the absence of a link to a specific terrorist act or acts

R.6 - Targeted Financial Sanctions

- Countries should implement targeted financial sanction regimes top comply with United Nations Security Council Resolutions relating to the prevention and suppression of terrorism and terrorist financing

R.30- Responsibilities of law enforcement and investigative authorities

- Designated law enforcement authorities have responsibility for ML and TF investigations
- In major proceeds of crime and TF generating offences law enforcement agencies should develop **proactive and parallel financial investigations**
- This should include when the predicate (original) crime is outside of their jurisdiction

- Countries should have the responsibility **to identify, trace, freeze and seize** property and assets suspected to be the proceeds of crime or TF and make them subject to confiscation
- Make use of temporary or permanent **multi-disciplinary groups** specialised in asset confiscation and financial investigation (Pakistan has developed the capacity for financial data warehousing under the National Counter Terrorism Authority (NACTA) to support financial investigations by LEAs and Intelligence agencies)
- Seek **cooperative investigations** in other jurisdictions

R.31 - Powers of law enforcement and investigative authorities:

- Law enforcement agencies should be able to gain access to all necessary documents and information for use in their investigations
- The existence of powers to require compulsory measures for the production of documents held by financial institutions and designated non-financial businesses and professions (DNFBPs) for the search of persons and premises and obtaining witness statements and the seizure of evidence, without the court order
- The ability to use a wide range of investigative techniques to proactively and reactively tackle ML and TF
- The ability to identify beneficial owners and assets without prior notification of the owner
- The ability to request all data held by the FMU (FIU in other countries)

A 'financial investigation' means an enquiry into the financial affairs related to a criminal activity, with a view to: ν identifying the extent of criminal networks and/or the scale of criminality; ν identifying and tracing the proceeds of crime, terrorist funds or any other assets that are, or may become, subject to confiscation; and ν developing evidence which can be used in criminal proceedings.

A 'parallel financial investigation' refers to conducting a financial investigation alongside, or in the context of, a (traditional) criminal investigation into money laundering, terrorist financing and/or predicate offence(s). Law enforcement investigators of predicate offences should either be authorised to pursue the investigation of any related money laundering and terrorist financing offences during a parallel investigation, or be able to refer the case to another agency to follow up with such investigations

Section 2 - Pakistan Relevant Legislation to Counter Terrorist Finance and Money Laundering

Following the attack on an Army Public School in Peshawar the Pakistani Government created the National Action Plan (NAP) to tackle the issue of terrorism. This included measures to combat terrorist finance. The following legislation is relevant to dealing with terrorist finance and money laundering cases.

2.1 Legislation

Anti- Money Laundering Act 2010

This enables the seizure of assets and cash involved in money laundering and financing of terrorism. This provides a framework for the search and seizure of property and assets linked to money laundering.

Section	Offence / punishment
3. Offence of money laundering.—	A person shall be guilty of offence of money laundering, if the person:— (a) acquires, converts, possesses, uses or transfers property, knowing or having reason to believe that such property is proceeds of crime; (b) conceals or disguises the true nature, origin, location, disposition, movement or ownership of property, knowing or having reason to believe that such property is proceeds of crime; (c) holds or possesses on behalf of any other person any property knowing or having reason to believe that such property is proceeds of crime; or (d) participates in, associates, conspires to commit, attempts to commit, aids, abets, facilitates, or counsels the commission of the acts specified in clauses (a), (b) and (c).
4. Punishment for money laundering.—	Whoever commits the offence of money laundering shall be punishable with rigorous imprisonment for a term which shall not be less than one year but may extend to ten years and shall also be liable to fine which may extend to one million rupees and shall also be liable to forfeiture of property involved in money laundering or property of corresponding value

Anti -Terrorist Act 1997

This covers the seizure of assets and property of persons involved in terrorism and proscribed organisations.

Section	Subject	Provision
6(7)	Definition of "Terrorist"	The term "terrorist" includes an individual who has been concerned in the commission, preparation, facilitation, funding or instigation of acts of terrorism;
11H	Fund Raising	A person commits an offence if he invites another person to provide money, receives money or other property or if he provides money or other property; and knows or has reasonable cause to suspect that it will or may be used for the purposes of terrorism.
11I	Use and possession	A person commits an offence if he uses money or other property for the purposes of terrorism; or possesses money or other property; and intends that it should be used, or has reasonable cause to suspect that it may be used, for the purposes of terrorism

Section	Subject	Provision
11J	Funding Arrangements	A person commits an offence if he enters into or becomes concerned in an arrangement as a result of which money or other property is made available or is to made available to another;
11K	Money Laundering	Retention or control, by or on behalf of another person, of terrorist property by concealment to be considered an offence
11N	Punishment under Sections 11H to 11K	Any person who commits an offence under sections 11H to 11K, shall be punishable on conviction with imprisonment for a term not less than five years and not exceeding ten years and with fine

Section	Subject	Provision
11B	Proscription of Organization	The Federal Government may list an organization as a proscribed organization in the First Schedule if there are reasonable grounds to believe that it is concerned in terrorism
11E	Measure to be taken against a Proscribed Organization	✓ Its offices, if any, shall be sealed ✓ All literature, posters, banner, or printed, electronic, digital or other material shall be seized; and ✓ any publication, printing or dissemination of any press statements, on behalf of or in support of a proscribed organization shall be prohibited.
11EE	Proscription of Person	The Federal Government may list a person as a proscribed person in the Fourth Schedule of ATA,1997 if there are reasonable grounds to believe that such person is concerned in terrorism, an activist, office bearer on an associate of an organization kept under observation under section 11D

Section	Subject	Provision
11EEEEE	Prohibition on disposal of Property	If the Investigation Team has sufficient evidence to believe that any property is likely to be removed transferred or otherwise disposed, the team may direct the owner not to remove, transfer or otherwise dispose of such property before an order of appropriate authority for its seizure is obtained.
11O	Seizure, Freeze and Detention	On proscription made under section 11B or 11EE, the money or other property owned or controlled, wholly or partly, directly or indirectly, by a proscribed organization or proscribed person shall be frozen or seized, as the case may be;
11OO	Access to Services, Money or other Property	The Federal Government may permit a person to make available to a proscribed organization or proscribed person such services, money or other property as may be prescribed, including such money as may be required for meeting necessary medical and educational expenses and for subsistence allowance.
11P	Attachment of a Terrorist Property	✓ An investigating officer may apply to a court for an order for attachment of a terrorist property. ✓ Any cash attached under this section shall be held in a profit and loss account and the profit and loss so earned shall be added to it on its release or forfeiture.

Foreign Exchange Regulation Act 1947

This regulation gives discretion to confiscate non-declared cash at borders. It is likely that terrorist groups will use cash couriers with no apparent criminal or terrorist links. This act provides the ability to seize cash at border crossings without having to prove terrorist links. This could be used with profiling to identify potential couriers.

Code of Criminal Procedure

S.51 Searching of arrested persons and S.523 allows the magistrate to make an order in relation to the disposal of the property

S.98 relates to searches of property suspected to contain stolen property, forged documents, etc.

Customs Act 1969

S.158 Power to search Persons

S.168 Seizure of items liable for confiscation

S.170 Police Powers and the disposal of property seized

Section 3 Understanding Money Laundering and Terrorist Finance

What is Money Laundering?

The object of laundering money is to get the financial benefit from criminality without being caught. The terrorist or criminal will always seek to avoid leaving a trail that can lead back to the original crime (predicate offence). The terrorist will also seek to conceal the origins of the money allowing it to be used to further terrorist activity or be re-invested to increase their funds.

Traditionally there is a three-step phase to money laundering, **placement, layering and integration.**

Sources of Terrorist Finance (not exhaustive)

- Extortion
- Robbery
- Smuggling, Counterfeit goods
- Drug Trafficking

Placement

Goal – Deposit Terrorist Finance into the financial system

- Change of currency
- Change to bigger notes
- Transport cash to other areas
- Cash deposits

Layering

Goal – Conceal the Origin of Terrorist Finance

- Wire Transfers
- Cash withdrawals
- Cash deposits in other accounts
- Split and merge with different accounts

Integration

Goal – Create the appearance that origin of money is legal

- Create fictitious loans, contracts, invoices
- Disguise ownership of assets
- Purchase property, assets
- Invest in legitimate businesses

The Placement Phase

This often the riskiest phase for the terrorist money launderer, as being caught with large amounts of cash can be difficult to justify. The placement phase is the initial act to get the money into the financial system. This could just be as simple as paying money into an account. Commonly a tactic called 'smurfing' is adopted, which is the payment of smaller amounts into multiple accounts to avoid drawing attention to the launderer. Many countries have amounts which require closer due diligence before they can complete the transaction, $10,000 is the US limit. So many launderers will make several random transactions (to seemingly unrelated individuals) under this figure to conceal the larger amount. A terrorist or criminal paying money into a Hawaladar to move it to another city is effectively placing it.

The Layering Phase

This is where the launderer tries to make it difficult for the investigator to trace the origins of the money. Generally, the launderer will try and move the funds through a series of transfers or conversions to make it difficult for the investigator to trace it. Layering will make it hard to identify and seize all the funds, so whilst some may be discovered some will probably get through. This may well entail jurisdictions that have weak AML controls. The cash could also be shown as payments for goods or services to make them appear legitimate.

The Integration Phase

Having moved the funds through the initial stages the launderer can now invest these funds in the legitimate economy. This could be through property purchases, luxury goods or investment in legitimate businesses. The fundamental aim is to legitimise the funds and prevent detection and seizure.

Limitations as to the Three Stage Model

The three-stage model relies upon their being a crime that produces the money or goods that need to be laundered. Sometimes the money can be lawfully obtained or earned. For example, a businessman makes a good profit on his business and the money is paid into his account. This money is legitimate. He then makes the decision not to pay his taxes and sends the money to an offshore account out of the country. The money has now become illicit, however it was already in the system and therefore there was no placement stage. It has gone directly to stage 2 layering!

This is also true with some terrorist money. Person A has got a job and legitimately earns money. He pays this money into his account. At some stage he is radicalised and joins a terrorist group he uses his money to rent a lorry and buy materials to make a truck bomb for his group. They go onto to attack a market and causes a great deal of damage and injury.

At what stage did his money become terrorist finance? It was lawfully earned and only when he decided to use the money to rent the van and buy materials for a bomb did it become terrorist finance. This would have been impossible for the banks or police to identify without intelligence that identified him as having been radicalised and intending to plan an attack. The same is true of charitable

donations. If the donor intends for the money to be used for a good cause like a hospital or building shelters for displaced persons, it is not terrorist finance. If the charity diverts this money to fund terrorist groups, it can be considered as terrorist finance. If the charity is a proscribed organisation, then donating to it is an offence and if any funds are identified they can be seized.

Section 4 - What are the Sources/Channels of TF

- The abuse of charities and charitable donations
- Self-financing (legitimate income)
- Funding from sympathisers or membership payments
- State Sponsoring
- Activities in failed states or safe havens (ISIS oil manufacture)
- Criminal Activities - Drug Trafficking, Kidnap, Extortion, Robbery & Theft, Smuggling and Counterfeiting
- Madrassas raising funds to support terrorist groups

Charities/Non-Profit Organisations (NPOs)

Potential forms of NPOs that exist in Pakistan

- Genuine NPOs seeking to provide assistance in areas of deprivation and need
- Sham NPOs – Set up fraudulently to provide a vehicle to move illicit funds in and out a country and support terrorist or criminal activities
- Service NPOs- These provide a service such as housing, social services, education, religious education and health care
- Expressive NPOs – These support the arts, sport and recreation.

NPOs sending funds to high risk countries pose a potential vulnerability that donations given in good faith may be misused when they reach their destination country.

Main Characteristics of High Risk NPOs

- Service style NPOs
- High cash intensity
- Public donations and membership fees main source of funds
- Support a particular religion
- Based in a provincial or capital city
- Operate in or send and receive funds in high risk jurisdiction
- Have relationship with organisation operating in High Risk Jurisdiction

Case Study 1

A domestic NPO raising funds for humanitarian relief in an area of conflict was collecting funds in donation boxes outside of religious institutions. The funds were then paid into a domestic bank account.

The founder of the NPO was suspected of diverting funds to facilitate terrorism rather than humanitarian aid. A law enforcement investigation resulted in the arrest of the founder of the NPO and the seizure of $60,000 from the domestic account.

Source FATF

Case Study 2

In response to a humanitarian disaster, a large international NPO was providing aid by way of cash payments to beneficiaries in areas controlled by a terrorist organisation. The NPO delivered the cash payments through a local money service business (MSB). An examination of the humanitarian relief programme, carried out by one of the NPO's partner organisations on its behalf, raised concerns. The examination revealed that in certain instances, the MSB was deducting a 'tax' to be passed on to a listed terrorist organisation. In other instances, the beneficiaries of the charitable funds were being 'taxed' by representatives of the terrorist organisation themselves following the receipt of the financial aid. The examination also found that there was a general understanding and acceptance that a portion of charitable funds would be diverted for terrorist purposes and that this was common practice amongst NPOs and related organisations working in the area. Following a joint investigation by the national NPO regulator, the national FIU and law enforcement, the NPO was advised of its responsibilities with regards to reporting such incidents, and was required to provide training to its staff to prevent future incidents.

Source FATF

Self-Financing

This is becoming increasingly common. Where states have effectively disrupted terrorist groups, fighters have often returned to their countries of origin and they have organised their own funding, planning and execution of attacks. In some cases previously unknown individuals have become radicalised and planned attacks. This presents significant problems for investigators trying to identify lone wolves or small cells. Many of the recent European attacks were self-funded with legitimate incomes or low-level criminality that would not have raised any red flags.

Case Study

UK – Salman Abedi a Libyan student living in Manchester funded a terrorist attack at a pop concert through a student loan of £7000 and housing benefit payments. He purchased the materials and constructed the bomb himself. The nature of how the funds were raised would not have raised any alarms with the authorities. He detonated the bomb killing himself and 22 people and injuring over 100 other members of the public.

Funding Through Sympathisers

Many communities donate to organisations that they know are fronts for terrorists either through fear of reprisals for not contributing or because that group has influence in the community in the absence of state support for social services or amenities. This support can also be provided by friends and family who sympathise with their cause.

Case Study

UK -Three people funded family members fighting for ISIS in Raqqa. They sold a BMW car, jewellery and obtained credit cards for their use. The funds of over £10,000 were sent through a high street remittance service to Syria.

They were sentenced to prison sentences from 4 years to 18 months

UK Daily Mail Report 2016

Safe Havens or Failed States

Terrorist groups flourish in areas with little or no law and order. In these areas they become the Government. They are then able to build training camps for their operatives, tax local businesses or exploit raw materials such as oil and mineral wealth.

Case Study

ISIS created an area or safe haven where they took over the banks seizing the money and valuables they found. They took over the production and sale of oil in the region and at the height of their power were assessed to be worth $2 billion. They attracted many foreign terrorist fighters to join their cause.

These territories have now largely been recaptured and IS were effectively defeated in a conventional conflict. Many of the FTF have now returned to their respective countries and this will create challenges for law enforcement to manage the spread of decentralised, small autonomous cells.

Criminal Activities

Drug Trafficking

Afghanistan is the major global manufacturer of heroin. There are at least 1.3m users in Europe with a growing number (8m) of users in Pakistan. There is always going to be a massive demand for heroin and therefore it will continue to be a major source of revenue in this part of the world. The growing and harvesting of the opium crop, the manufacturing process and the supply routes and workforce are all protected by terrorist groups for a source of the revenue. This yields vast sums of cash that require laundering to avoid detection.

Case Study

In Colombia FARC was heavily involved in the cocaine trade to raise significant funds for their cause. They protected the factories and clandestine landing strips in the jungle. They liaised with other criminal gangs in to facilitate and control the drugs distribution in return for a share of the profits. They also liaised with other terrorist groups such as the Irish Republican Army and ETA a Basque separatist group from Spain over urban terrorist techniques.

Kidnapping

This is the source of revenue for many terrorist groups. The ability of armed groups to kidnap journalists, aid workers and affluent locals is a constant problem. Families will often be prepared to sell assets to meet the demands and some foreign governments have paid very large sums for the release of their citizens. These kidnaps can often become a criminal terrorist nexus as hostages are bartered over and swapped. Large sums of cash are often handed over and require laundering and dispersing around terrorist organisations and sympathisers.

Case Study

Karachi Oct 2018 3 Daesh suspects were arrested by the Anti Violent Crime Cell (AVCC) for the kidnap of a young man from Gulistan-e-Jauhar. A ransom of 10m rupees was demanded from an Afghan cell phone. The family paid the ransom and a financial investigation linked it to 35 separate bank accounts that had been used to transfer funds to Daesh in Afghanistan. Two cloth traders were also arrested for having also moved funds to Daesh via Hawala dealers. This group was also linked to bombings in Mastung and Quetta.

Source - Dawn News Pakistan

Extortion

In areas where law and order has broken down it is easy for terrorist groups to exert influence on the local communities. They are able to tax local businesses through direct demands or payments to move goods through checkpoints. The access to utilities such as water and electricity can also be controlled. Failure to comply with these demands can be met with violent punishments.

Case Study

In Peshawar 2015 many businesses received extortion demands from phones with Afghan SIM cards. Some businesses and individuals that failed to pay demands suffered attacks with grenades and small IEDs. The CTD believes that these demands are from groups based in Afghanistan. The Pakistan Telecommunications Authority is currently working on blocking unregistered phones.

Source – South Asia Terrorist portal SATP

Case Study 2

In 2008 Chiquita a company in the worldwide trade of bananas admitted the payment of extortion demands to the US Justice Department. They admitted paying $1.7 m to AUC a Colombian terrorist group responsible for many serious atrocities. They also stated that they had paid ELN and FARC (two other prominent terrorist groups) as control of the banana growing area shifted.

They were fined $25m and placed on probation for 5 years and agreed to implement a compliance and ethics programme. They were faced with a difficult choice either pay up or risk there employees or infrastructure being attacked, or selling their holdings at a considerable loss. However, paying extortion demands invites other terrorists to repeat the activity. Chiquita made a decision to admit to previous activities and change future behaviour.

Robbery and Theft

With the existence of armed groups the likelihood of robberies is increased. Terrorist groups have routinely robbed banks to fund their operations. If funds are drying up terrorists will often resort to robbery of business premises such as banks for cash, or stealing cars at gunpoint (car-jacking). These offences are made easy by the fact that the terrorist groups have access to weapons and operatives who are prepared to use them.

Case Study

In the first 6 months of 2013 The Mujahadin of Eastern Indonesia robbed 1.8 billion rupees from a series of bank, gold store, phone shop, money service business robberies. This was as a result of other funding streams drying up through the arrest of leading members of the group and the reluctance of communities to contribute for fear of arrest by the authorities.

Source – South Asian Terrorist Portal SATP

Smuggling

The Pakistan border with Afghanistan is over 2000 kilometres long. The Northern territories reach up to China. It is estimated that the Pakistan Government loses $2.6 billion of revenue through the smuggling of 11 types of legitimate goods such as TVs, phones, car parts, diesel and cigarettes. These smuggling routes are well established and whatever goods are in demand will be smuggled to order. The routes will almost certainly pass through areas controlled by terrorist groups who will demand payment for safe passage or simply take over the smuggling routes for themselves.

Smuggling is extremely lucrative and flexible. As soon as a product is taxed heavily it becomes a commodity to smuggle. The porous borders and law enforcement coverage over such a large area make this activity a profitable source of income.

Case Study

November 2018 Customs officials in Quetta raided a train and found it full of smuggled goods, such as carpets and other household essentials. The goods had been well concealed within the train. The concealment showed that this well organised and all the available space had been packed with goods.

The police were not able to catch the smugglers, again showing their caution and ability to evade detection. – Source Dawn News

In 2016 Pakistan lost $2.63 billion of revenue from the smuggling of household goods such as TVs, car parts, diesel, tyres, mobile phones and tea amongst other items.

Counterfeit Goods

The revenue from counterfeit goods is now more than illegal drugs. 80% of counterfeit goods are believed to come from China. This includes pharmaceutical products and a recent report from the Pakistan Government estimated that up to 50% of pharmaceutical products were counterfeit. This poses a massive health risk to the public and a massive source of revenue for criminals and terrorists who get involved in the trade.

Case Study

Case Study

The terrorists responsible for the Paris attacks in 2015 raised funds through drug trafficking and the sale of counterfeit goods including Nike shoes.

The Belgium city of Molenbeek is home to a disproportionately large number of people who sympathise with Islamic terrorism. They are in turn associated with the sale of counterfeit goods. In 2012 3 tons of counterfeit clothes and accessories were seized by the authorities. UNIFAB said 'Law enforcement agencies in France and abroad need to stop treating counterfeiting as a 'petty crime' and understand that it bankrolls terrorist activity.'

UNIFAB report commissioned by French Government 2016

Fraud

With the increased ability for consumers to borrow money and get credit there are opportunities for this to be exploited. 'Break out' frauds are becoming increasingly common. A person opens accounts with a bank and initially runs the account in profit showing normal usage. Then having created the perception of being a normal customer applies for loans and credit cards. These are then taken up to the limit and the cash withdrawn and the customer disappears with the money.

Case Study

In 2017 a 27 year old woman of Pakistani origin Zoobiah Shahnaz living in the United States raised over $85,000 through a series of loans and credit card usage, known as a 'break out fraud' to purchase bitcoins. This was to cover the money trails.

She then transferred this money through a series of transactions to China, Pakistan and Turkey in smaller amounts to avoid raising any red flags.

She then quit her job and booked a flight to Islamabad via Turkey. She was arrested at the airport by US authorities.

She was found guilty of money laundering, conspiracy to launder money and bank fraud and faces a lengthy prison sentence

Source - International Business Times 2017

Credit Card Fraud

The internet offers the potential to anonymously purchase stole credit card details. These are then used to make purchases and sell on goods. The IT skill of many terrorist organisations allows funds to be gathered in this way. It can also be done in different countries and the money transferred to where it can be used for operations or logistical support.

Case Study

YounisTsouli a UK citizen who called himself 'Irhabi 007' and Tariq al –Dar acquired stolen credit card data from the web, using online forums such as Cardplanet. When they were arrested al Dar had got 37,000 stolen card numbers on his computer which they had used to make $3.5 m worth of purchases. Tsouli used 72 cards to register 180 websites hosted by 95 different companies which were used to launder the proceeds of their crimes.

Human Trafficking

In recent times conflict zones and extreme poverty have led to unprecedented numbers of people leaving their own countries in the search of work and a better standard of living. Many of these people seek a better life in European countries. However, the routes to get there involve long and dangerous journeys across seas and deserts and the need to get across protected borders. A massive industry has evolved to provide this service involving transportation routes and carriers and false documentation. With people prepared to stake all their wealth to make these crossings, a large number of criminals and terrorists have become involved in this activity. Nearly all countries are involved as a destination, stopover or transit point. This again generates huge amounts of cash that needs to be laundered. All countries are affected by this activity.

Case Study

Boko Haram leader Abubakar Shekan threatened to sell 276 girls kidnapped from a boarding school in Chibok Nigeria. He said, “there is a market for selling humans, Allah says I should sell. He commands me to sell. I will sell women.”

UNICEF say that 1.2 million children are trafficked annually. Trafficking helps demoralise enemies and can be the source of fighters.

Source - Homeland Security News Wire 2014

Antiquity Thefts

ISIS took control of heritage sites such as Palmyra and supervised over its partial destruction and the looting and sale of valuable artefacts. Many of these artefacts reached art sales across the world and have made significant profits. A go between in Syria and Turkey claimed to have sold one piece for $1.1m.

Pakistan - Potential Money Laundering Methods/Channels

- Layering and structuring payments to come in under reporting restrictions
- Refining – Changing small bills to large ones
- Expensive Asset Purchases – Luxury goods, vehicles and property
- Currency Exchange – Purchase of foreign currency
- Hawala
- Wire Transfers
- Postal orders
- Mobile banking apps – Easypaisa, Omni UBL
- Gambling at Casinos
- Legitimate Business – Invest in local business and divert profits back into funding terrorism
- Charities and Madrassas – Channelling charitable donations to terrorist groups

Section 5 - Power of Investigators in Money Laundering and Terror Financing Cases

Powers under AMLA 2010

Relevant Section of Law	Power and Role of Investigators
Section 8 - Attachment of property involved in money laundering	• The Investigating Officer (IO) on the basis of a report from an investigating or prosecuting agency • By order and prior permission of the court • May provisionally attach a property which he believes is involved in ML • For a period not exceeding 90 days • Within 48 hrs the IO must submit a report and copy of the order to the head of the relevant investigating or prosecuting agency in a sealed envelope • Interested persons or occupier may remain on premises • Monthly progress reports to the court
Section 9 - Investigation	• Within 7 days of the attachment or seizure of property under sec 14 and 15 • The IO shall serve a notice on the interested person to disclose in not less than 30 days the sources of income, earnings or assets or by which means he/she acquired the property • The notice requires the person to show cause why the property should not be forfeited to the Federal Government • The IO believes that the property has been involved with ML he can apply to the court for an order confirming the attachment • If the court having heard the evidence from the concerned person decides that the property was concerned in ML it can issue an order confirming the attachment and the IO can take possession of the property. • The IO can then seek authority from the court for the sale of the property

Section 13 Power of Survey	• Where the IO is in possession of evidence that gives him reason to believe that ML offences have been committed • He may with permission of the court enter any place within the area assigned to him • He may require the proprietor or employee present to facilitate inspection of records, check transaction details and supply relevant information • The IO must then submit a report within 48 hours to the relevant head of the investigating or prosecuting agency in a sealed envelope • The IO may mark documents, remove copies and record statements of any person present
Sec 14 – Search and Seizure	• If from information held the IO has reason to believe a person has committed a ML offence or is in possession of any property involved in ML or any record relevant to ML proceedings • He may authorise a subordinate officer to i) enter and search any building place or vessel, vehicle or aircraft ii) Force entry iii) Seize property iv) Mark or take away copies of records v) Make an inventory of property vi) Powers are conferred by authority of court, **unless urgent then it can be authorised by an officer not below rank of BS-20** vii) Submit a report within 48 hours to the head of the relevant investigation or prosecuting agency viii) If the IO believes that evidence may be tampered with, he may seize material he believes may be relevant. The reasons for the seizure must be recorded
Sec 15 Searches of Persons	• If the IO has reason to believe has any items secreted about their person relevant to the investigation • He may search that person and seize any relevant property • Report to head of relevant investigation or prosecuting agency within 48 hours • Females may only be searched by female officers • IO to record property found

Sec 16 Power of Arrest	• If the IO has reason to believe a person is guilty of an offence under the act • He may apply for a warrant from the court • Report to head of relevant investigation or prosecuting agency within 48 hours • Within 24 hours (excluding travel to court) of arrest the person must be taken to a judicial magistrate
Sec 17 Retention of Property	• Under sec 14/15 the IO can retain property for 90 days • The court will need to be informed about property that requires appropriate directions, such as perishable goods that may need to be sold to avoid financial loss. • Retention beyond 90 days requires authority of the court
Sec. 18 – Retention of Records	• Under Sec 14/15 records may be retained for 90 days • Retention beyond 90 days requires the authority of the court
Sec. 24 - Appointment of Investigating Officers	• The Investigating or prosecuting agency may nominate an IO from their own officers • The Federal Government may nominate an IO by special or general order of a level of BPS-18
Sec.25 Authorities to Assist	• Officers of the Federal Government, Provincial Government, Local Authorities and Financial Institutions shall provide requisite assistance to IOs • Whoever wilfully fails or refuses to provide such assistance shall be proceeded against by its respective department or organisation
Sec.27 Letter of Request to Contracting State	• Where an IO believes that evidence is required in connection with an investigation under the act • He may with the authority of the head of the relevant agency • Issue a letter of request to the competent authority in the contracting state • To investigate or take steps requested in the letter of request • Evidence collected shall be deemed to be evidence collected in the course of the investigation
28. Assistance to a contracting State in certain cases.—	• Assistance can be provided to another state following a Federal Government request in response to a letter of request
Sec.29. Reciprocal arrangements for processes and assistance for transfer of accused persons.—	• Deals with the issue of summons to produce documents or arrest or search warrants

	through as request of a contracting state through the Federal Government
32. Punishment for vexatious survey and search	• An officer found guilty of a vexatious survey or search • Is liable to a term of imprisonment of 2 years or a fine of 50,000 Pkr
41. Act not to apply to fiscal offences	• Without prior consultation of the FMU the IO shall not charge anybody with ML when the predicate offence is a tax offence (Sales Tax Act 1990 or Federal Excise Act 2005)

Powers of Investigators under ATA 1997.

Relevant Sections of ATA 1997	Brief Summary of Investigators Powers
9. Power to Enter & Search	• Officers having reasonable grounds for suspecting that a person hjas possession of written material or recordings contrary to S.8 of the act • May enter to search and seize such material • Prior to entry they must make a written record of their reasons • This must be provided to the person or premises searched
10. Power to Order Forfeiture	• Following the commission of S.9 offence • Power to forfeit any material identified in the investigation
11EEE. Power to Arrest and Detain Suspect Person	• Power to arrest and detain persons included on the list at S.11EE • Subject to authority the suspect may be held for 12 mths
11EEEE Preventative Detention for Inquiry	• Any persons suspected to be involved in terrorist activity under the act may be detained for 3 months (Extensions possible) • Authority of officer of not below Superintendent or through a JIT • Subject must be produced at court within 24hrs of detention
11EEEEE Prohibition of Disposal of Property	• Officer not below rank of superintendent or JIT • May serve notice on the subject of an investigation under this act • Not to dispose, transfer or sell any property
11L Disclosure of Information	• A person commits an offence if he fails to disclose to a police officer • The fact that somebody has committed an offence under the act • Defences under this section are explained

11M Cooperation with Police	• No offence under S.11H to 11.K if acting under the consent of an officer of rank not below rank of Dep. Superintendent
11P Application to Attach Property	• An officer may make an application to the court for the attachment of a terrorist property • Any cash seized will be held in a profit or loss account • If acquitted the defendant shall be repaid in full with any interest accrued
21E Remand	• The court may authorise the detention of a suspect for 30 days • Can be extended to 90 days in total • Suspect must be brought before the court within 24 hours of detention excluding travelling time
21EE Power to Call Information	• A superintendent of police or equivalent rank of other relevant agency or JIT • May call for information from a person • Or require them to deliver documents or material or examine any person • May require a bank of financial institution to provide any information held by them
27 Punishment for Defective Investigation	• Any officer found out to having failed to conduct an investigation diligently or properly May be subject to punishment by the courts
27AA Punishment for False Implication	• An officer who falsely involves, implicates or arrests any person under the act • Can be punished by 2 years imprisonment and /or a fine • Government approval is required before action is taken under this section
27B Conviction on the Basis of Electronic or Forensic Evidence	• A conviction may be secured on the basis of electronic or forensic evidence • Or other evidence that may have been obtained by modern devices • As referred to in Article 164 Qanun-e-Shahadat 1984 • Provided that the court considers the evidence to be genuine

Section 6 – Gathering Evidence and Conducting Financial Investigations

61 Sources of Intelligence

- Police
- LEAs
- FMU
- FIA
- Credit Reference Agencies
- Provincial/District Authorities
- Land Registry
- Directorate of Immigration and Passports
- NADRA
- Ministry of Information and Heritage
- Banks and Financial Services Sector
- Merchant Services Providers
- Retailers
- Open Source Data

Police

6.1.1 Intelligence Reports

- Provide start points for financial investigations.
- Links to other terrorists or associates who could be laundering money.
- Reviewing existing police intelligence will identify and gaps that the enquiry team may have. Financial investigation can help reduce these gaps.
- Community intelligence crucial to understanding grass roots methods for money laundering
- Intelligence sharing by all stakeholders under NACTA platform

6.1.2 Arrest Reports

- Associates arrested at the same time
- Property in their possession
- Location of arrest
- Nature of criminality
- What account did they give as to their involvement in the alleged offence?
- Details of persons arrested for terrorism are maintained on the NACTA database

6.1.3 Source/Agent/Informants Information and Recruitment

- Very cost-effective way of policing
- Financial informants can provide information that can be corroborated and tracked to identify networks and associations with targets
- Can the FI identify somebody in an organisation that could be recruited or is a key member of the group

- If the source is involved in financing of terrorism, they must be debriefed or handled by somebody who is financially aware
- Can the source be tasked to obtain financial information.
- Is the source aware of what they can and can't do. Do they have terms and conditions or rules of engagement
- Never act on single strand intelligence that may compromise your source.
- Use financial investigation as a way of paralleling information in order that it can become actionable intelligence and not compromise origins of the information.

6.1.4 Debriefing Prisoners

- Where a terrorist is already in custody, have they been debriefed with a view to understanding the financing and operational activity of the group?
- Financial Investigators can become involved or provide questions to help in tracing TF and people concerned
- Cooperation can be rewarded without drawing attention to the prisoner
- Who is the terrorist sharing a cell with? Do they have information?
- Who is visiting the prisoner?
- Aspirationally, all debriefs should contain a section that deals with finance and sources of wealth to build on the overall picture of TF.

6.1.5 Other Law Enforcement Agencies

- Anti-Narcotics Force - Drug Trafficking is a huge Criminal Terrorist Nexus and most drugs trafficking jobs will have a terrorist crossover. It is imperative to have an excellent liaison with this team.
- The FIA has national reach and involvement in many areas of criminality and will provide a valuable source of liaison, expertise and intelligence
- The Military and Military Intelligence may form part of a Joint Intelligence Team and will have good sources of intelligence and will be able to provide security if searches in difficult areas are required.
- Border Authorities are a valuable source of intelligence and can provide excellent intelligence on the movements of suspects and goods to establish financial patterns
- In border areas between provinces liaison officers in the other provinces should be able to assist with criminal groups who frequently cross borders and areas. Criminals rarely pay any attention to borders in rural areas. This can lead to administrative problems for investigators. Anticipate this and establish a system for fast time intelligence sharing and identify liaison officers

6.1 6 Financial Monitoring Unit

- Handles all Suspicious Transaction Reports/Suspicious Activity Reports
- Currency Transaction Reports
- Wire Transfers
- Cross border reports
- Currency transaction reports by casinos

- These are all valuable start points for financial investigations
- Financial Investigators need to use this database as a proactive as well as a reactive investigative tool
- Information from the FMU will have come from the banks therefore it may not be held on police or law enforcement databases. It is often the case that phone numbers provided will be accurate and current as they are kept as 'clean phones'
- SARS should always be checked at the beginning of an investigation as it may reveal information that is valuable to an enquiry
- As the size of the database grows so does its value as a key research tool.
- This must be a strategic consideration and mainstay of private/public sector engagement for the future
- The scope of the FMU has been enhanced to be able to access detailed financial information from the banks databases

6.1.7 Financial Investigation Agency

Federal Agency with national coverage of numerous areas including borders, corruption and copyright theft amongst other areas. They will have expertise in different areas that can assist provincial investigations.

The FIA will respond to the following referrals and reports

i) Suspicious transaction reports (STRs) and cash transaction reports (CTRs)
ii) Private Complaints (whistleblowers)
iii) LEA referrals involving TF
iv) Border Control Authority referrals
v) NCB and Interpol referrals
vi) International Request
vii) Federal Government referrals

The FIA verifies information from anonymous sources and can convert them into enquiries. The enquiry is conducted under Inquiry and Investigation Rules (2002) and FIA SOPs. The FIA has the power to summon witnesses and requisition bank records and relevant documentation. The Enquiry Officer then submits a Confidential Final Report for consideration of the FIA Scrutiny Committee. If there is evidence to support a case it is registered as an FIR. If not, it is closed or referred to another unit if offences other than terrorism are identified for them to investigate.

The FIA have powers to investigate apart from ATA 1997 and AMLA 2010, such as Prevention of Electronic Crimes Act 2016, Protection of Pakistan Act, Pakistan Penal Code 1860, Code of Criminal Procedure 1898 and FIA legislation. On completion of the investigation a report will be submitted to the relevant court under sec.173 Code of Criminal Procedure.

The FIA utilises a diverse range of intelligence sources many already referred to in this manual, including The Pakistan Telecommunications Authority (PTA) for SIM card and call data records, income tax data from the Federal Board of Revenue.

The following databases are also used;

- Schedule IV – Police
- UN Lists – FIA,NACTA & SECP
- Red Book – FIA
- Kalkan FTF and Pace Maker – NCB & FIA
- Passport Verification – DGI & Passport authority
- Other Proscription Lists – MOI & Home Departments

The FIA liaised extensively with police units and military and inter services intelligence. They are able to initiate enquiries into NPOs, NGOs, Madrassas and Trusts. They are able to seek third party value assessments of such organisations. They are also able to probe the origins and destinations of funds if they go abroad through MoI and MoFA and follow up on foreign enquiries.

6.1.8 Credit Reference Agencies (PACRA)

- Financial history
- Names of financial associates
- Address check
- Electoral roll data
- Insurance information
- Cars hire purchase agreements
- Properties
- County court judgements
- Credit searches and phone numbers
- Credit reference agencies will require a yearly subscription fee and are hold sometimes sensitive data. All checks need to be linked to a recorded financial enquiry in order that they can be audited in the future. This is key to maintaining integrity and public confidence that a potentially intrusive form of monitoring is being lawfully used.
- Remember if somebody is no trace on the credit reference database , it means they have not applied for anything that requires credit such as loans, a bank account with an overdraft. This could mean that the person is careful to avoid debts. It could also mean that they are taking steps to protect their anonymity.
- It is appreciated that in Pakistan that not that many of the population hold bank accounts. However, this is likely to change and in the next 5-10 years it is anticipated that 100m Pakistanis will have bank accounts or mobile accounts. Credit reference agencies will therefore become more important in gathering intelligence.

6.1.9 Merchant Service Providers

- These are very important sources of information for investigators. It may be that there is a liaison with each of the providers and you must ensure that you follow the correct protocols in contacting them. Otherwise they could quickly become overloaded with requests and this could affect the working relationship

- However, they will have significant information and they will be able to tell you what they are capable of. The will have the following information.
- Account information
- Application forms
- Address and DoB
- Telephone numbers
- Credit card details
- Expenditure
- IP addresses
- In some cases they may be able to provide an IP history

6.1.10 Provincial and District Authorities

- Housing Benefit
- Land and property tax.
- Amount of time person has lived at an address.
- This information becomes important when you are establishing somebody's legitimate lifestyle when assessing any criminal/terrorist benefit

6.1.11 Land Registry

- Property owned
- Value of property – Many online sites will tell you what houses or flats have been sold for or purchased.
- Mortgages on property. Who holds the mortgage, can you see the beneficial owner?
- Land Records as well as details of luxury vehicles Purchased

6.1.12 Directorate of Immigration and Passports

- Name
- Gender
- Place of birth
- Addresses
- Passport number
- Names of family members
- Method of payment for passport
- This all valuable information in preparing a profile and can identify other lines of enquiry.
- Travel history – Where have they travelled to and how often

6.1.13 NADRA

- To obtain one of these card you have needed to have provided a number of documents to confirm your identity.
- They will hold family data too
- These cards are relied upon with their 13 digit number to open bank accounts and register phones.

6.1.14 Banks and Financial Sector

- All banks should have a police liaison role. They will be able to tell you what they can provide – Under ATA and with the powers of the Joint Investigation team the bank must release financial information to you when requested.
- Generally, they will not give information unless they have a court order
- On receipt of a production order they will provide you with account data.
- Account monitoring orders will allow you to get a daily update on the conduct of an account, so you can monitor activity as it takes place. If you request this service, ensure that you are in a position to use it and review it.
- In exceptional circumstances they may be able to provide live updates of ATM withdrawals this may only be true of major banks with a dedicated police/fraud liaison tea.
- They will often have client files where they have asked security and customer due diligence questions. These can be very detailed and they will show interesting facts as to how they intend to use their accounts or how much money they expect to earn and save. From these records you may be able to establish what their outgoings are and the source of their funds.
- This data will enable you to establish their legitimate income
- This can then be compared to their outgoings and if there is a disparity that is where you will establish their criminal benefit
- A full disclosure will enable you to see loans, business associates and IP addresses
- If it doesn't look right it generally isn't. Don't be afraid to ask questions until you can see the validity of the transactions or business. If an account is turning over significant profits in excess of what they had anticipated it needs a closer look, to see that the credits are from a genuine source. If you are unsure ask somebody familiar with banking products being used by the suspect.
- Large and frequent cash deposits need to explained and accounted for.
- You must also be aware that the banks will be sensitive if they have allowed criminal activity to have taken place when they should have reported it to the FMU. If it is a major breach you should bring it to the attention of your supervisor as it may need further dissemination to Federal Authorities.
- Remember that many suspects will use family members to bank their criminal or TF money to distance themselves from any criminal activity. Make sure that you check family and married names of female relations.

- Always handle material from the banks with care. Banking secrecy is closely guarded by the financial sector. Therefore, all material you receive from the banks should be securely stored and not disseminated to anybody outside of the enquiry team. If the material is highly sensitive (involvement of politicians or religious leaders for example) there should be an inclusion list of who has been allowed access to it.

- If possible, request material in an electronic format as you will be able convert it to an excel spreadsheet which makes analysis and research significantly easier. Some banks do this routinely others will supply you with paper files. It is possible to purchase software that converts this to excel spreadsheets. If you have a major enquiry this will be a consideration.
- At the conclusion of enquiry if possible, let the financial institution know the result and where their assistance was valuable, make reference to it. This improves relationships with the financial sector and will make future liaison better.

6.1.15 Retailers

- Dates and times of purchases
- Expenditure
- Possible CCTV
- Loyalty card data – Sometimes when the suspect uses cash they will want to redeem points with the loyalty card. This enables the investigator to see how much money the suspect is spending.

6.1.16 Open Source

- Facebook, Twitter, Instagram, Linked In, YouTube and other social media
- Blogs
- Media articles
- Google and other major companies in this field are becoming increasingly detailed in the material they collect from their subscribers. They will see your internet searches and activity and if you have geotagged photographs they send adverts to you that their systems have calculated will be more likely to have impact with you. Essentially it is all about selling you more! Can police utilise this thinking for criminal investigation?

6.2 Developing a Financial Strategy

In all investigations into terrorist finance/serious crime there should be a financial strategy. In many cases financial investigations should run parallel to the main investigation, but at the outset of the investigation the financial investigator should have a meeting with the lead investigator and determine what lines of enquiry are being conducted and where financial investigation may add value. The financial investigator will be in a position to explain what a financial profile can contain. The FI should request the following information;

- What information do they hold on the subjects of interest already?
- What information are they seeking to progress the enquiry and why?
- Will the information be required on an intelligence basis or for evidential purposes? (Where it is required for evidence banking details will have to be obtained via production orders).
- If confiscation of assets is being considered restraint orders will need to be prepared to prevent the dissipation of assets and cash.
- If witnesses are being sought, the FI may be able to assist.

Financial enquiries may also identify persons subject to financial difficulties, who may be in a position that they be approached to assist the police with their enquiries.

- How they want the information/evidence disseminated and in what format
- What tactics will develop the financial enquiry, production orders from the banks, surveillance (conventional or intrusive), tasking informants, interviewing witnesses, overseas intelligence/enquiries, intelligence led targeted cash seizures.
- Agree tactics in line with resources and objectives.
- The final strategic plan should identify your objectives and the tactics you intend to use and a brief rationale so if the case is handed over another FI will be able understand

6.3 Identifying Potential Targets

Terrorist groups are comprised of several levels and some of these roles may be combined

- Fundraisers
- Facilitators/Logistics/Technical experts
- Operatives
- Controllers/commanders
- Donors

It is unlikely that you are able to combat all these levels in one approach. It is also difficult to get straight to the controllers and it often requires the targeting of lower level members of a group to incriminate the controllers. This is where it is important to work out tactics that will provide a chance of gathering evidence to identify and implicate members of the group and identify assets.

Proactive tactics include;

- Target cash hides
- Identify and stop couriers
- Financial orders to identify accounts of fundraisers/logistics members
- Surveillance to identify physical assets, properties and association
- Searches of peripheral group members to gain intelligence and evidence against the more established members of the group
- Target businesses or remittance services that are believed to be assisting in the laundering of terrorist finance using other regulations to disrupt the flow of funds.
- Task informants to infiltrate groups especially in relation to terrorist finance.

Example of selective tactics

UK Police - Identified cash couriers through analysis of phone data and Automatic Number Plate Readers. Through this analysis they created opportunities to stop these couriers when they were likely to be carrying cash using uniform patrol officers so as not to compromise the source of intelligence. This led to significant cash seizures and arrests of couriers resulting in more senior members of the crime groups having to courier cash personally and providing law enforcement with arrest opportunities.

6.4 Surveillance

- All surveillance should have objectives, surveillance for surveillance sake is expensive and a potential waste of resources. When the surveillance has met the days objectives it should be terminated. Lengthy aimless surveillance raises the risks of compromise and setting back an investigation.
- To ensure best value an FI should do prior enquiries on the subject. This can reveal the most appropriate day to monitor activities, places visited, associates, shopping habits and general lifestyle and days when the subject is more active, and surveillance is likely to reveal more information
- During live surveillance if possible, an FI should be contactable to run live checks on premises visited and persons associated with. This can provide the team with valuable intelligence and may affect the nature of the surveillance.
- Any use of an ATM machine should be marked by one of the team using a disclosable card. This will identify the users account details and provide evidence directly associating a suspect with an account. If that account is being used for TF, offences may already have been committed.
- Times of phone calls should be noted for time and duration, these could be linked to transactions later and you will have direct evidence as to who was using the phone at the time
- Rubbish bins are valuable sources of intelligence and the surveillance team should seek to not only recover discarded receipts, but also identify which rubbish bin the subject uses for repeat recovery.
- Tracking devices are a cost-effective way of monitoring the activity of a target vehicle and can be monitored live time or historically from an office. This can be linked with banking information and CCTV footage to identify and confirm the movements of a target.
- Officers need to be trained in the deployment and use of this equipment.
- If no FI is available during the surveillance, they should be made aware of what has happened in order that they can run financial checks on persons and places to develop new leads. The FI must be instrumental in requesting this information to stay informed of the direction of the enquiry to ensure that no financial leads have been missed.

6.5 Searches

- Searches are a key part of any police enquiry. Searches for financial investigation are no exception and must be planned carefully.
- Firstly, you should ensure that the search warrant is correctly obtained and the material you are seeking is listed on the warrant. Make sure that you have possession of the warrant and that you can serve it on the occupant.
- Ensure that you have completed a risk assessment and checked on the neighbourhood and the threats posed by the occupants or neighbours. Local police should have community intelligence or threat assessments for the area. If the area is hostile, you will have to liaise

with the army or local police to ensure that they can provide a protective cordon so you can search the premises in safety. They may only be able to provide this cordon for a limited time, so you will have to conduct your search with this in mind.

- Prior to the search you will need to have established who is responsible for what role. Who is serving the warrant and will identify as the officer in charge, exhibits officer, arresting officer, searching officers, security and other persons that may be necessary to include on the warrant. For example you may need an IT expert or an accountant to attend business premises.
- If you are searching a property and you expect to find legal professional privilege material you need to have a plan to deal with. It may be that you take an independent lawyer with you or you seal the material in a non-transparent bag and get an independent lawyer to review it later.
- When on premises you need to conduct a methodical search to ensure that nothing is missed. Decide on who will search what room. If property is found ensure that it is recorded at the time.
- If permitted by law, it is good practice to record answers to any property recovered at the time. The suspect will not have had time to consider his answer. If asking questions about financial matters they will often talk to you. These answers can often be very relevant when reviewed later.
- If cash is found on the premises it must be dealt with professionally. Ideally you should not count it, as depending on the amount it may take a long time, or if you get the amount wrong you could be accused of theft. The money should be sealed in a tamper proof bag and signed by the finding officer and countersigned by the exhibits officer. The Suspect should also be asked to sign it and to say how much there is present if they know. Best practice is that the cash is double bagged to prevent any allegations of tampering.
- This money can then be counted on return to a secure location and if a controversial case or a significant amount of money, it is advisable to video the recovery at the scene and during the count and show the bag being resealed to avoid allegations of impropriety.
- You should anticipate the quantity of material you are likely to find. For example, if it is a working business there will undoubtedly be paper records, but also the potential for data to be stored on computers/printers. If you are expecting to find computers make sure they have been listed on the warrant. It is also advisable to take a computer expert with you to assist in the recovery of relevant evidence.
- Having seized the computers have you the ability to search the data that is held on them again be prepared to take advice. One of the biggest issues is the volume of material that can be stored on modern systems. You may not have the ability review all the material. In one recent case the Serious Fraud Office in the UK said it would have taken a team of 6 lawyers 10 years to review recovered material.
- If the premises are a working business, you may have to shut it down. There may be a cost implication in doing this that if you do not charge the occupant with an offence you may have to pay costs. If you are intending to arrest the owner but wish for the business to continue working you will have to consider taking somebody who is able to make provision for the business to be maintained. This, in itself, can be expensive, but it may allow people to carry on working and maintain the value of the business. This important if you wish to use this a part of the future asset confiscation.
- All evidence taken from the premises will need to be correctly listed and the chain of evidence recorded to show how it was transported to the police station or storage facility.

- If the search is of a sensitive or controversial nature (community or religious leader) it may be advisable to film the premises prior to the search being conducted and at the conclusion to show transparency and reduce the potential for complaints to be made.
- During the search it is good practice to record the details of the entrances, locks security features such as CCTV or lighting, points you can access the building without being seen, persons on premises, plan of the building, sleeping quarters and any safes or secure internal store rooms. This will be of value for anybody seeking to raid the premises in the future or seeking covert entry. This must be recorded on an intelligence report.
- If you anticipate female occupants you should have female officers on the search team in order that all occupants on premises can be searched without causing offence.

Checklist (not exhaustive)

Research and Risk assess	Be prepared for what you might find
Warrant	Check validity and accuracy
Roles and Responsibilities	Brief all involved- check understanding
Other staff	Do you need specialists such as IT experts/Forensic accountants
Photograph/video	Evidential and protection from allegations of damage/theft
Cash	Packaging – security and integrity
Chain of evidence	Record and register
Question and answer	Record comments and any admissions contemporaneously
Intelligence Report	Record details of premises, locks, access etc and persons on premises

6.6 Undercover/Covert Operations

- These can be very low level such as test purchases/donations with marked money with a view to identifying cash flows later or testing to see what financial assistance a money service business is prepared to provide. Do they ask for identity or ask where the source of funds is from. If they do not the chances are that they are prepared to launder money. This could then result in the use of legislation to fine them or seek to close them down. This activity could be used to target certain areas to make it more difficult for terrorists to launder their money.

- All operatives must be fully trained and the operation authorised and risk assessed at the appropriate level
- Undercover officers with skills in financial affairs are in short supply and it is sometimes better to use agents who work in these areas. However undercover officers provide better evidence at court. It is also possible to use agents to introduce undercover police officers to groups enabling them to infiltrate them.

- Controlled deliveries such as the ones used by the ANF to capture drug traffickers may be modified to incriminate terrorists. Careful planning and research of intelligence is required in any such operation.
- Sting operations are effective and have been used in many jurisdictions. Again these need careful planning and risk management, but often provide excellent intelligence and evidence. The US law enforcement agencies are experienced at setting up fake businesses to attract criminals to come to them. This can mean setting up physical business premises or online engagement offering money laundering services. In either case these need to be planned and authorised having taken into consideration legislative issues and the safety of undercover officers.
- Covert internet investigators are becoming very important and the internet offers safe access to sites used by criminals and the ability to converse with them and identify potential risks, patterns of criminality and suspects operating in your jurisdiction. This use of the internet is becoming increasingly significant, but will need careful planning to ensure that it is lawful and appropriate in the circumstance. The IT access will also become an issue as internet access will need to be from a non-police computer as criminals and terrorist are able to use software that can track who has been looking at their websites and conversing with them online.

6.7 - Financial Profiles

A financial profile of a subject can vary in depth and detail. This will have to be agreed with the investigation team at the outset of the case. They should all follow the same structure. The main subjects of the investigation should have full profiles created, especially when confiscation is being considered.

The following is a list required for a financial profile. Depending on the circumstances as agreed with the enquiry team this could be varied or expanded upon.

- Bank account details
- Any other accounts with financial institutions such as savings accounts
- Business/company accounts
- Real estate owned or controlled
- Share and stock portfolio owned or controlled
- Other assets owned or controlled
- Offshore asset owned or controlled
- Vehicles/vessels or aircraft owned or controlled
- Legitimate income
- Overall income
- Overall expenditure

From this profile it should be possible for the FI to make an assessment of the subject's net worth. From the information obtained the FI will make an assessment of the terrorist funds available or connected to the subject. This will be presented to the court to determine what assets should be subject of a confiscation order. In the pre-trial phase it will also justify the police requesting restraint orders (attachment of property) to prevent the subject dissipating his/her assets.

The expression owned or controlled is a key question. Surveillance may reveal that the subject has exclusive use of property or assets. In this case the court may take a view whether these assets fall under the confiscation order.

6.7.1 Company Profiles

As criminals and terrorists become more sophisticated in their activities it is likely that companies will be used to conceal their laundering and terrorist financing methodologies. The following is a non-exhaustive list of information categories that could be relevant in criminal and terrorist investigations;

- Company or business details (name, incorporation date, type of business, company business registration number)
- Nominated positions in the company, Owners, directors and secretary with associated details name, date of birth, address, salary and duration of employment.
- Shareholder details and their share allocation
- Business structure and composition
- Information can be obtained from the Securities and Exchange Commission of Pakistan

6.8 Interviews

In all investigations interviewing of suspects and witnesses is a key component. Interviews should be planned and prepared to ensure that the interviewer has access to all the relevant information and has structured the interview to cover all the relevant areas.

The PEACE model is a simple structure to conduct interviews.

P - Plan and prepare, make sure all the information, exhibits are available, plan structure for you interview and a list of questions you want to cover

E – Engage and explain, spend some time to develop a relationship with the interviewee and make them relax as much as possible. Explain what will happen in the interview

A – Account and clarify – Try and elicit an account from the interviewee to explain the points you have identified in your plan. Financial questions will often be answered as the majority will be seen as routine. Challenge any inconsistencies to ensure that you understand the answers given.

C – Closure – End the interview and explain what will happen next

E – Evaluate – Review all the answers and decide if a further interview is required to clarify any points or issues

In relation to financial interviews the following areas should be covered

- Assets owned or controlled by the subject eg Cash held in accounts, shares, property and valuables.
- Liabilities such as mortgages, loans, overdrafts and credit owed
- Source of funds – Salary, interest, inheritance, rental income, gifts etc
- Expenses - Loans and mortgages, household bills, travel expenses and other repayments

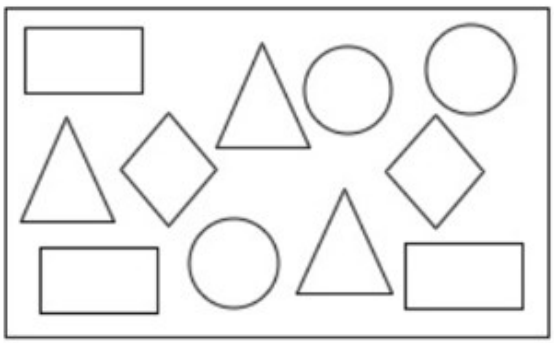
The questions required to ascertain a full understanding are detailed and it is worth pre-planning them

- Salary from who, for how long and how much?
- Assets – From who, how much, how did you pay and proof of purchase
- In relation to mortgages and other debts – What was the original debt, how much is owed still, who the lender was, documentation available, how was the loan spent did you provide a security for the loan?
- Business connections and associates
- Nature of business and trading links outside of country

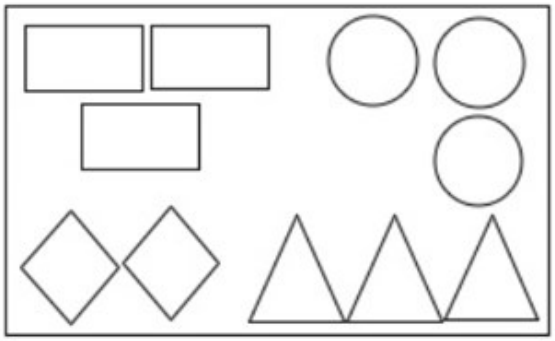
Ensure you follow a checklist for the interview that you have prepared and discussed with colleagues prior to interview if possible. If you have a complex interview with several topics to cover, consider how you might break the interview down into smaller sections. It may be a chronological approach and following a timeline might work. However, if the interview is about several businesses you may have to deal with them all separately.

Breaking the interview into smaller parts is called 'grouping' or 'chunking.' This will allow you to develop a systematic approach to the interview and cover all the topics in a structured way. This limits the chances of missing out areas of questioning.

Grouping



Example 1



Example 2

6.9 Forensic Accountants

In complex cases and especially ones involving business accounts it is advisable to seek the assistance and direction of a forensic accountant. What do they provide?

- Expert witnesses and qualified accountants, experienced at auditing and accounting for businesses or charities like the ones you are investigating.
- Examine and analyse and compare financial material to ensure facts and figures are correct and consistent with the business under investigation.
- Produce material for interview, investigation and court proceedings. The key aim is to make it understandable for somebody with no financial background.
- Explain financial material recovered to investigators and prosecutors

When conducting searches of accountant's premises subject to any investigation, forensic accountants should be contacted in order to ensure that the correct material is sought and seized. Such as the following.

- Statutory Accounts - that contain company balance sheet, profit and loss accounts, cash flow statement and director's report
- Client money accounts – These are where businesses lodge money with an accountant for business purposes such as a property sale.
- Working papers – These should reflect the business being undertaken and detail transactions.
- Client records and notes

It is appreciated that the services of forensic accountants may only be available for complex investigations. However, in high profile or sensitive cases their assistance and input can be extremely valuable in both identifying assets and identifying terrorist funds, criminal and bad practice that may well prove an offence.

6.10 Inter-Agency Co-operation

This may be on an informal basis between units or neighbouring provinces or other government agencies. Or through more formal arrangements. The FIA has access to many other agencies that can facilitate the collection of data to assist financial investigations.

Joint Investigation teams

The JIT was devised to ensure that all investigative/operational opportunities were considered in the investigation of terrorist offences.

- To perform joint financial investigations with all terrorist investigations
- To identify all sources of TF irrespective of monetary value
- To identify all persons involved in TF – donors, fundraisers, facilitators and operatives
- Identify all assets that may be subject to forfeiture, freezing/restraint and ultimately confiscation
- To identify the latest TF typologies
- Apart from other offences of terrorism which the JIT may be looking at, the following terrorist financing offences under Anti-Terrorism Act, shall be specifically taken into account;

  i. **11H. Fund Raising** for the purpose of terrorism or by a terrorist or organization concerned in terrorism.
  ii. **11I. Use and Possession of Money or other Property** for the purposes of terrorism.
  iii. **11J. Funding Arrangements** as a result of which money or other property is made available or is to made available which may be used for the purposes of terrorism.
  iv. **11K. Money Laundering** to facilitate retention or control, by or on behalf of another person, of terrorist property.
  v. **11N. Punishment** under Sections 11H to 11K may be for a term not less than five years and not exceeding ten years and with fine.

  - Section 21EE of the ATA, empowers the Superintendent of Police during the course of investigation, with the permission of the Anti-terrorism Court, to require any bank or financial institution to provide any information relating to any person, including copies of entries made in the bank's or a financial institution's records, including information of transactions saved in electronic or digital form which are reasonably believed to be connected with commission of an offence under ATA.

6.11 Phases of Financial Investigation

1. Open, Plan and Register
2. Conduct Investigation

3. Judicial Phase
4. Confiscation and Disposal

Phase 1 – Open, plan and register – Parallel Investigations

Register the investigation (FIR or alternative record). It is important that all financial investigations are recorded in order that figures can be compiled to work out where they are being undertaken and to demonstrate that all opportunities to combat terrorist finance are being taken up.

At the beginning of the investigation it is a valuable exercise to establish which agencies and police units could offer assistance or provide intelligence.

The planning will involve intelligence gathering and it may be apparent that the target is involved in other criminality other than terrorism. It is at this stage that you need to consider if it would be easier to prove other offences. For example, it may be smuggling, this would therefore involve the Border Force, customs and dependent on the goods being smuggled agencies involved in tackling counterfeit goods. Having gained evidence that the subject's money has come from illicit activity money laundering offences can be pursued and confiscation proceedings planned. It is crucial that all the intelligence is evaluated for accuracy. It is also important to check that the targets of you investigation are the ones that present the greatest threat in line with your threat assessments. Use your resources to target the most serious offenders.

Parallel Investigations

The planning stage is critical to establish roles and responsibilities of all involved in the investigation and decide who is leading the case, Senior Investigating Officer. At the outset of the terrorist investigation **all opportunities to trace money flows and individuals involved in funding must be exploited through parallel investigations**. An operational plan should be drafted in order that resources and timescales are considered and a financial strategy is completed to ensure all opportunities for cash seizure and confiscation have been identified. If a complex case this plan must be signed off by a supervisor. Intelligence gaps need to be identified and a plan to address them considered. Initial tactics should be decided on and consequences anticipated. Contingency plans need to be in place if the initial plan does not progress the enquiry.

All these activities need to be risk assessed and if the risks are higher than acceptable a plan must be considered to mitigate them.

Checklist

1.Evaluate Intelligence

2.Register FIR or alternative record

3.Identify Agencies or Authorities that may have a shared interest

4.Identify relevant offences – These may not be ATA offences

5.Complete initial collection plan to identify evidence required and potential intelligence/evidential gaps.

Phase 2 - Conducting the Investigation – Proactive Financial Investigative Options

Despite the planning and the tactics, it is possible that it does not run to plan. The investigation will need to be evaluated at regular intervals to ensure that it is progressing. All officers involved should be briefed properly and able to put forward their ideas and intelligence that they may have uncovered. The SIO should establish when and where the meetings should be held and decide on when full meetings or supervisors' meetings are necessary.

Proactive Financial Investigative Tactics - If the chosen tactics are not providing the necessary evidence are there different tactics that can be used. Are there different subjects that could be investigated with a view to getting an insight into the main targets. Can informants be re-tasked to get new information are there undercover options? The manual identifies a number of **proactive financial investigative options** available to the Investigating Officer. These should be adopted where operationally feasible. No investigative plan should be complete without considering **any opportunities for cash seizure and identification of terrorist assets, irrespective of monetary value.**

The sophistication and value of the target will dictate the length of time that the investigation may take.

If the case is complex do not be afraid to seek advice from subject matter experts. Other agencies or professionals may be able to assist.

If the case is complex, consider taking early advice from prosecution lawyers as they will be responsible for prosecuting the case and they may have some directions as to what evidence will provide the best chances of a successful prosecution.

Ensure that record-keeping and the storage of evidential material is considered at the start of the enquiry. If the enquiry is protracted a system for keeping the material will be invaluable when you have to review intelligence and evidence. The format of the files should follow an accepted protocol so that each case has a common structure and if investigators have to change the new investigator will be familiar with the landscape of the investigatory filing.

This will also be key when preparing the case files for the judicial phase. Throughout the collection of evidence ensure that all assets are identified that may become subject to confiscation. It will be necessary to liaise with prosecutors to ensure that the correct papers have been prepared. To achieve maximum impact it is desirable to serve attachment or restraint orders at the time of arrest. This also prevents the suspect from taking steps to hide or sell these assets.

Checklist

1.Evaluation and review meetings organised

2. Ensure parallel financial investigation has been started to supplement the main investigation

3.Brief officers of roles and responsibilities

4.Change Tactics if required

5.Seek expert advice (Forensic accountants, prosecutors)

6.Maintain decision logs

7.Maintain a storage system and record for documents and exhibits

8. Prepare Financial Profiles - Business and Personal

9. Ensure all assets have been identified and papers have been prepared for restraint (attachment)

Phase 3 - Judicial Phase

In complex cases hopefully, you will have had the opportunity to consult with a lawyer to ensure that you have built a solid case.

Consultation and case conferences are especially valuable to ensure that the evidence is available in a legible and presentable format. It may be that the lawyer identifies some gaps in the evidence, you may be able to take further statements or obtain other material that could bridge this gap.

Witnesses need to be protected and their safety and security considered prior to the court case. How will they get to and from court, can we protect identities if required?

In major cases when there are multiple accounts and a significant volume of transactions it may be appropriate to seek the assistance of a forensic accountant. They are able to explain money flows to the lawyers and also help with clarifying complex financial issues for presentation at court. If you can't explain it clearly it is going to be difficult to prove your case in a criminal court.

The case is not concluded at the time of the arrest and it may be that other information becomes apparent that will identify further suspects or evidence.

Checklist

1.Consultation between Police/LEAs and prosecutors

2. Design presentation of case to ensure clarity and understanding

3.Identify any evidential gaps

4.Witness liaison and witness safety considerations

5.Specialist Assistance for complex cases – expert witnesses

6.Ensure all assets have been identified and orders served on interested parties

Phase 4 - Confiscation and Disposal

If the defendant is convicted, you now need to concentrate on confiscation.

Hopefully you have already identified his assets and accounts holding any money or shares. The court will be able to make an order to have these assets confiscated. Confiscation is important for two reasons firstly you recover money to repay victims and also recover money for the State. Secondly you ensure that the individual or his organisation are deprived of funds that they could use to further their cause and fund future attacks.

Defendants will employ any tactics not to pay any orders made by the court. As the officer in the case you must ensure that the confiscation is pursued. This can be time consuming and may involve more court appearances. The owners of the property will try to pass ownership of the property to another or claim that assets are now gone. There is no substitute for determination in completing this part of the enquiry.

If the order is realistic and the assets are present a determined long-term approach should see results. There is a danger in falsely assessing their benefit and placing an unrealistic order on the defendant. This will make recovering the order difficult and leave an unresolved order on record which makes the police and prosecution appear inefficient. This will also stand out on future FATF mutual evaluation reports.

Checklist

1.Create a plan and timeline for confiscation and try to stick to it

2. Be prepared for defendant's efforts to delay or frustrate the process

3.Make sure that any confiscation order is realistic and that you have identified the assets correctly

4.Ensure that all results are recorded

5. Where appropriate seek authority to publicise significant cases. This is to emphasise law enforcement successes and to highlight the message that crime and terrorism does not pay

6. If assets are identified abroad consult with prosecutors and explore bilateral agreements and Mutual Legal Assistance Treaties

Section 7 – Foreign Assistance in Financial Investigations

In many complex investigations the money trail will lead to foreign jurisdictions and territories. International and inter-agency cooperation is a significant requirement for FATF.

The investigation should not finish if evidential and financial trails leave Pakistan. Prosecutors will be able to advise on legal requests through bilateral agreements or Mutual Legal Assistance Treaties. There will be a format for these requests that the prosecutors can assist with. Any requests for intelligence and evidence will need to be authorised by the senior officer leading the enquiry.

Confiscation enquiries will often lead to other countries. In the current climate of anonymous beneficial ownership many countries will assist in returning enquiries. In some cases they may even restrain property and assets enabling Pakistan to seek confiscation proceedings.

Organisations such as FATF can provide information about international enquiries and assistance. Interpol is also a very useful point of contact to enable Pakistan to identify and liaise with the relevant police departments who can assist with such enquiries.

Extradition of suspects for offences committed in Pakistan will require liaison with the prosecutor to ensure that a proper application is completed to satisfy the requirements of a foreign jurisdiction. If the offence committed in Pakistan is an offence in the other country there is a possibility of securing an extradition. Issues may arise if the offence is one that attracts the death penalty. If the country is one that subscribes to the European Court of Human Rights they will not allow the extradition of a suspect that may face the death penalty.

Section 8 - Training and Methodology

- Practical Exercises – Class based exercises to support modular based learning and presentations
- Lectures – Based on needs analysis of CTDs. SMEs to deliver lectures/presentations on relevant topics
- Workshops – Designed to meet identified learning needs and supported by class exercises

UNODC
United Nations Office on Drugs and Crime

Plot # 5-11, Diplomatic Enclave, G-5, Islamabad, Pakistan
Tel: +92 51 2601461-2 Fax: +92 51 2601469
Email: unodc-pakistanfieldoffice@un.org
Website: http://www.unodc.org/pakistan