TOOLKIT ON AML/CFT IN PAKISTAN

VOL. I

Operational Guidelines for the Investigation & Prosecution of Money Laundering & Terrorism Financing Offences in Pakistan
TOOLKIT ON AML/CFT IN PAKISTAN

VOL. I

Operational Guidelines for the Investigation & Prosecution of Money Laundering & Terrorism Financing Offences in Pakistan
CONTENTS

ABOUT THE TOOLKIT

TABLE OF AUTHORITIES

TABLE OF ACRONYMS

GENERAL EVIDENCE KEY

MONEY LAUNDERING AND TERRORISM FINANCING OFFENCES

1. Fund Raising (Section 11-H, Anti-Terrorism Act, 1997)
   a. Text of the Provision
   b. Ingredients of the Offence
   c. List of Relevant Evidence

2. Use and Possession (Section 11-I, Anti-Terrorism Act, 1997)
   a. Text of the Provision
   b. Ingredients of the Offence
   c. List of Relevant Evidence

3. Funding Arrangements (Section 11-J, Anti-Terrorism Act, 1997)
   a. Text of the Provision
   b. Ingredients of the Offence
   c. List of Relevant Evidence

4. Money Laundering (Section 11-K, Anti-Terrorism Act, 1997)
   a. Text of the Provision
   b. Ingredients of the Offence
   c. List of Relevant Evidence

5. Support to Proscribed Organizations (Section 11-F(5), Anti-Terrorism Act, 1997)
   a. Text of the Provision
   b. Ingredients of the Offence
   c. List of Relevant Evidence

6. Violation of UN Security Council Resolutions (Section 11-OOO, Anti-Terrorism Act, 1997)
   a. Text of the Provision
   b. Ingredients of the Offence
   c. List of Relevant Evidence
7. Offence of Money Laundering (Section 3, AMLA)
   a. Text of the Provision
   b. Ingredients of the Offence
   c. Predicate Offences
   d. List of Relevant Evidence

INVESTIGATION PROCESS CHARTS AND EXPLANATIONS

Terrorism Financing: Investigation and Prosecution Process Chart Explanation
1. Designated Law Enforcement Agencies (LEAs)
2. Information of an Offence
3. Opening an Inquiry
4. Registration of FIR
5. Initiation of Investigation
6. Conducting Arrest, Remand and Detention of Accused
7. Collection of Financial Record
8. Inter-Agency Coordination
9. Expert Analysis and Findings
10. Ascertainment of Relevant Sections of Offence to be Charged
11. Submission of Report u/s 173 CrPC.
12. Trial Stage

Money Laundering: Investigation and Prosecution Process Chart Explanation
1. Designated Law Enforcement Agencies
2. Initiation of Action
3. Registration of FIR
4. Ascertainment of Property Identified
5. Investigation Team
6. Special Procedure under AMLA 2010
7. Investigation Procedure
8. Collection of Record/Financial Investigation
9. Establishing the Offence of Money Laundering
10. Inter-Agency Coordination

GUIDELINES FOR TYPES OF EVIDENCE

Code A: Confessional Statements
Code B: Prosecution Witness Statements
Code C: Financial Record
Code D: Expert Analysis and Findings
   D1: Interception and Surveillance
   D2: Digital/Cyber Evidence
   D3: Additional Guidelines on Digital Forensics and Evidence
   D4: Forensics: Fingerprints and Handwriting
Code E: Additional Evidence Concerning Relationship with Proscribed Organizations

ANNEXURES

ANNEXURE I: TEMPLATES FOR WITNESS STATEMENTS
   a. Template to Record Statement under Section 161, CrPC.
   b. Template to Require Attendance at Investigations
ANNEXURE II: TEMPLATES TO OBTAIN FINANCIAL RECORDS

a. Template for Application to the Court for Want of Bank Record
b. Template for Letter to Bank for Want of Record
c. Template for Letter to all Banks to Identify Bank Accounts
d. Template of Letter to Obtain Record of Income Tax etc. from FBR
e. Template of Letter to Obtain Record from Excise Department
f. Template of Letter to Obtain Record of Immoveable Properties
g. Template of Letter to Obtain Record of NPOs
h. Template of Letter to Obtain Records from NADRA
i. Template of Letter to Obtain Records from DG-IMPASS
j. Template of Letter to Obtain Records from FIA- Integrated Border Management System (IBMS)

ANNEXURE III: TEMPLATES FOR EXPERT ANALYSIS AND FINDINGS

a. Template of Letter to Obtain Call Detail Records (CDR), etc.
b. Template of Letter to Obtain Forensic Analysis of Digital Equipment
c. Template for Application to Court for Social Media Applications Record
d. Template of Letter to Obtain Record from Social Media App Authorities etc.
e. Template of Letter to Obtain Expert Opinion on Fingerprint and Handwriting
Since Pakistan’s ‘grey-listing’ by FATF in June 2018, the State has attempted to adopt a holistic, whole of government approach in upgrading its AML/CFT legal and regulatory regime. While Pakistan is now deemed compliant on 24 out of its 27 action points after extensive legislation and administrative/regulatory reform, the remaining points require Pakistan to ‘demonstrate’ efficacy of its new processes. Thus, Pakistan will now have to ‘demonstrate’ that mechanisms it has put in place for identifying TF/ML activity are actually effective, that targeted financial sanctions are quickly and effectively applied to designated entities and individuals and that the criminal justice system is effective in enforcement of these regimes, from investigation to prosecution.

This is a daunting challenge, given that Pakistan’s criminal justice system in general is plagued by antiquated laws and procedures as well as a poor track record of investigation and prosecution. The nature of terrorism financing and money laundering today requires expertise in specialist investigative techniques and reliance on evidence that goes beyond traditional ocular testimony and confessions. Further, the wide-ranging nature of the new legislation and the powers it confers on various entities needs to be thoroughly understood by those to whom it applies for effective enforcement.

The Research Society of International Law (RSIL) has played an active role in developing domestic capacity with global CT and AML/CFT regimes in Pakistan over the past two decades. Since Pakistan’s grey-listing by FATF in June 2018, RSIL’s research team has dedicated thousands of hours to improving the State’s capacity in AML/CFT through the development of training guides, policy briefs, legal memorandums, podcasts and has conducted dozens of trainings and events in all four provinces of Pakistan for hundreds of investigators, prosecutors, judges, civil and military officials.

Through this process, RSIL identified the need to develop tools which delineate the various types of evidence which is available to investigators in Pakistan in AML/CFT offences, assist investigators in assessing the utility of such evidence for effective investigations and subsequent trial of the accused, guide investigators on the process of requesting or collecting such evidence and building a case based on such evidence.

RSIL’s research and engagement in this area further indicated that the investigators and prosecutors do not explore the broad spectrum of financial information which can be used as potential evidence during ML/TF investigations. Moreover, even
when that information is obtained, investigators, prosecutors and judges often lack the necessary skills and knowledge to understand the information provided. Hence, there was a need to develop detailed operational guidelines to obtain financial information from different sources, analyze it for red-flags/discrepancies which may assist the investigation, prosecution and adjudication of the case, and outline the legal processes through which this information can be lawfully obtained.

To this end, RSIL constituted two Working Groups, consisting of investigators, prosecutors and judges from all provinces as well as legal and financial consultants, to support and guide the development of an AML/CFT Toolkit. Working Group 1 (WG1) consisted of justice sector actors and legal experts from across the country and was mandated to develop general operational guidelines for the effective investigation and prosecution of AML/CFT cases in Pakistan. Working Group 2 (WG2) was mandated to focus on financial evidence in AML/CFT cases, and consisted of financial experts, professional accountants, bankers, tax lawyers and representatives of federal agencies with an AML/CFT mandate.

The two WG convened twice in Islamabad for two-day sessions in February-March 2021. This Toolkit consolidates the exhaustive and wide-ranging feedback from both WG and is divided in two volumes.

**AML/CFT TOOLKIT VOLUME I**

**Volume I** of the AML/CFT Toolkit focuses on specific ML/TF offences within the domestic legal framework in Pakistan, and sets out operational guidelines for the investigation and prosecution of these offences. In particular, it contains the following information:

**ML/TF Offences:**
- The legal reference and text of each ML/TF offence under Pakistani law.
- The ingredients of each ML/TF offence, including its *actus reus* and *mens rea* elements.
- A list of different types of evidence that may be relevant for the investigation of those offences.
- A list of common predicate offences to money laundering and their ingredients.

**Guidelines for Investigation and Prosecution of ML/TF Offences:**
- Investigation process charts for ML and TF under Pakistani law and their explanations.
- A description of each type of evidence:
  - Confessional Statements
  - Prosecution Witness Statements
  - Financial Records
  - Expert Analysis and Findings
  - Additional Evidence Concerning Relationship with Proscribed Organizations
    - The admissibility and evidentiary value of each type of evidence under Pakistani law.
    - General guidelines to collect, preserve and analyze each type of evidence.
    - Annexures containing template letters to request and record different types of evidence from various sources under the domestic legal framework.

**AML/CFT TOOLKIT VOLUME II**

**Volume II** of the AML/CFT Toolkit lays a special emphasis on the broad range of financial evidence which can be used as potential evidence during ML/TF investigations. In particular, it contains the following information:

- An introduction to financial evidence relevant to ML/TF investigations and navigation guide for the document.
- A comprehensive summary table of financial records and documents relevant to ML/TF investigations, their source, and the relevant information contained in them.
- A description of different sources of financial evidence in Pakistan:
  - Securities and Exchange Commission Pakistan
  - Federal Board of Revenue [Income Tax; Sales Tax; Excise Tax; Pakistan Customs]
  - Financial Institutions
  - State Bank of Pakistan
WORKING GROUP 1: PARTICIPANTS LIST

The first Working Group of justice sector actors consisted of investigators, prosecutors and judges from across Pakistan, as well as AML/CFT experts from the public and private sector. This Working Group contributed to the development of Volume I of the AML/CFT Toolkit. The Working Group had two, 2-day in-person meetings in Islamabad in which they added substantial value to Volume I of the toolkit, including identifying ML/TF offences and drafting guidelines for the collection and analysis of different types of evidence.

The participants included the following:

1. Mr. Muhammad Shahid Shahfiq, District & Sessions Judge/Senior Faculty Member, Sindh Judicial Academy
2. Mr. Muhammad Kaleem Khan, District & Sessions Judge ATC, Sahiwal
3. Mr. Rashid Mustafa Solangi, ATC Judge, Karachi
4. Mr. Sohail Jabbar Malik, District & Sessions Judge/ATC Judge, Karachi
5. Mr. Ejaz Ahmad Buttar, Additional District & Sessions Judge ATC, Lahore
6. Mr. Kamran Adil, DIG Headquarters, Islamabad Police
7. Dr. Ayaz Khan, Director Research & Analysis, KP CTD
8. Mr. Khan Zeb Khan, SP CTD, Peshawar
9. Mr. Khurram Saeed Rana, Deputy Director, Financial Investigation Unit, CTW, FIA Islamabad
10. Mr. Muhammad Mahfooz Kayani, DSP CTD, Islamabad
11. Mr. Rana Yasar, Inspector CTD, Gujranwala
12. Mr. Mukhtiar Ahmed, Director General Prosecution, Khyber Pakhtunkhwa
13. Mr. Atiq ur Rehman, Director Prosecution, Khyber Pakhtunkhwa
14. Mr. Abubakar Nauman Kazmi, Deputy Prosecutor General, CPD Lahore
15. Mr. Tahir Kazim, Deputy Prosecutor General ATC, Rawalpindi
16. Mr. Bakht Baidar Khan, Senior Public Prosecutor ATC, Swat
17. Mr. Talib Hussain Siyal, Assistant Prosecutor General, Sindh
18. Mr. Akbar Dad Babar, State Counsel High Court, Balochistan
19. Mr. Adnan Imran, Director Policy & Strategy, Financial Monitoring Unit, Islamabad
20. Ms. Samina Chagani, Deputy Director, Financial Monitoring Unit, Karachi
21. Mr. Israr Ahmed Khan (PSP), Director LEAs, NACTA
22. Mr. Nadeem Akhtar Sherazi, Director CFT, NACTA
23. Mr. Ifikhar Ahmed Khan, Deputy Director, LEAs, NACTA
24. Mr. Saad Hasan, Advocate High Court
25. Mr. Bakht Baidar Khan, Senior Public Prosecutor ATC, Swat
WORKING GROUP 2: PARTICIPANTS LIST

The second Working Group of Experts consisted of representatives of relevant investigation/prosecution agencies including NAB, FIA, Provincial Prosecution departments, Police etc., representatives of major private banks, professional accountants and tax lawyers and consultants. This Working Group assisted in the development of Volume II of the AML/CFT Toolkit. The Working Group had two, 2-day in-person meetings in Islamabad in which they added significant value to Volume II of the toolkit, including identifying relevant authorities to obtain different kinds of financial information as well as specific documents that can be used as financial evidence for ML/TF investigations, their relevance and descriptions.

The participants included the following:

1. Mr. Muhammad Shahid Shaﬁq, District & Sessions Judge/Senior Faculty Member, Sindh Judicial Academy
2. Mr. Kamran Adil, DIG Headquarters, Islamabad Police
3. Mr. Riaz Muhammad, Additional Director, Directorate of Intelligence & Investigation, Inland Revenue, Islamabad
4. Mr. Khurram Saeed Rana, Deputy Director, Financial Investigation Unit, CTW, FIA Islamabad
5. Mr. Faizan Ahmad, Deputy Commissioner, Corporate Zone, FBR, Faisalabad
6. Ms. Haleema Qasim, Deputy Director (CBCM), Directorate General of Investigation & Intelligence, Islamabad
7. Mr. Hafiz Muhammad Azeem Razzaq, Deputy Director, NAB HQ, Islamabad
8. Mr. Ch. Muhammad Jahangir, Director, Centre for Professional Development of Public Prosecutors, Lahore
9. Mr. Abubakar Nauman Kazi, Deputy Prosecutor General, CPD, Lahore
10. Mr. Manzoor Alam Khan, Senior Public Prosecutor, Peshawar
11. Ms. Sumera Baloch, Additional Director, Financial Monitoring Unit, Karachi
12. Ms. Noor-us-Sahar, Assistant Director, Financial Monitoring Unit, Islamabad
13. Mr. Saif ul Islam, Former Managing Director, Bank of Khyber, Peshawar
14. Mr. Arif Khan, Head International Compliance, LEAs Coordination & CFT Desk, Bank Al Falah, Karachi
15. Mr. Syed Yousuf Saeed, Head Anti Money Laundering, Habib Bank Limited, Karachi
16. Mr. Shiraz Maqbool Elahi, Head CFT Desk, HBL, Karachi
17. Mr. Muhammed Farooq Sarwar, Branch Manager, Silk Bank, Islamabad
18. Mr. Imran Mahmoud, Vice President/ Unite Head Legal Affairs, Muslim Commercial Bank, Islamabad
19. Mr. Jamil Akhtar, CEO, RSM Pakistan
20. Mr. Syed Tauqeer Bukhari, Advocate Supreme Court, Islamabad
21. Mr. Sarjeel Mowahid, Partner ABS & Co., Islamabad
22. Mr. Jahanzeb Durrani, Corporate Lawyer & Advocate High Court
23. Mr. Saad Hasan, Advocate High Court, Islamabad

EXTERNAL CONSULTANTS

RSIL also engaged the services of consultants including legal and financial experts to contribute to the drafting as well as the review of the AML/CFT Toolkit. They include the following:

1. Barrister Salman Safdar, Advocate Supreme Court, Pakistan.
2. Mr. Jamil Akhtar, CEO, RSM Pakistan.
4. Mr. Saad Hasan, Advocate High Court, Islamabad.
5. Daud Aziz Khokhar, former Head of Regulatory & Sanctions Law Division, ABS & Co.

We are especially grateful to our external consultants whose dedicated efforts were instrumental in improving the accuracy, usability and utility of the Toolkit.
RSIL TEAM

The RSIL team substantially contributed to the development of the AML/CFT Toolkit, and was responsible for incorporating all comments, changes and additions suggested by the Working Groups and External Consultants. The RSIL team that worked on the Toolkit includes the following:

EDITORIAL TEAM

1. Jamal Aziz, Executive Director, RSIL
2. Muhammad Oves Anwar, Director Research, RSIL
3. Zainab Mustafa, Deputy Director, RSIL
4. Fer Ghanaa Ansari, Research Associate, RSIL
5. Noor Fatima, Research Associate, RSIL

WORKING GROUP SECRETARIAT

1. Shayan Ahmed Khan, Senior Research Associate, RSIL
2. Abraze Aqil, Senior Research Associate, RSIL
3. Zoha Shahid, Senior Research Associate, RSIL
4. Mohib Wazir, Communications and Outreach Associate, RSIL
5. Aimal Amjad Quraishi, Research Associate, RSIL
6. Awais Ahmed Ghori, Administrative Officer, RSIL
TABLE OF AUTHORITIES

CASES

Abdul Hadi vs. The State, 2016 PCrLJ Note 70
Abdul Manan vs. State, 2017 PCrLJ QHC
Adnan Hafeez vs. The State, PLD 2016 Lahore 318
Asim Nawaz alias Kaleem Nawaz vs. The State, 2019 PCr.LJ 920
Badru l Haq (PLD 1963 SC 704)
Bahader Khan vs. The State, 2012 PCrLJ Pesh. 24
Ghulam Umer Memon vs. Jabbar Satti, PCr.L.J 2016 IHC 1103
Happy Manufacturing Co. vs. FBR, 2019 PTD 1922 LHC
Ishtiaq Ahmed Mirza vs. Federation of Pakistan, PLD 2019 SC 675
Ishtiaq Ahmed vs. Federation of Pakistan, PLD 2019 SC 675
Jawad Ayoub vs. Muhammad Farid 2005 PCr.LJ 129
Kareem Bukhsh vs. The State, 2017 YLR 1779
Kashif Anwar vs. Aga Khan University, YLR 2013 KHC 2294
Law Society of India vs. Fertilizers and Chemicals, AIR 1994 Ker 308
Manthar Ali vs. S.H.O, 2013 PCrLJ 553
Manzar Masood vs. Bank Islami Pakistan Ltd. 2017 CLD 1947 Kar
Maryam Nawaz Sharif vs. Chairman NAB, PLD 2020 Lah 205
Mazool Hussain vs. Abid Hussain, PLD 2008 SC 571
Mobashar Ahmad vs. State, 2009 SCMR 113
Mohsin Ali Shah vs. S.H.O Police Station Gargh Maharaja, 1995 MLD 771
Muhammad Asghar vs. Hamza Ilyas, PLD 2019 Azad Kashmir High Court 35
Muhammad Bilal vs. Superintendent of Police, Dera Ghazi Khan, PLD 1999 Lah 297
Muhammad Farooq vs. Sana Rizwan, PCr.L.J 2018 KHC 1676
Muhammad Hani vs. The State, PLD 1993 SC 895
Muhammad Irfan vs. the State, PLD 2015 Lahore High Court 78
Muhammad Latif vs. Statem, 2008 PLD SC 503
Muhammad Latif vs. State, 2008 PLD SC. 503
Muhammad Mohsin Ghuman & others vs. Govt. of Punjab, 2013 SCMR 85
Munas Parveen vs. Additional Sessions Judge PLD 2015 Lah 231.
Nasir Ahmad vs. State, 2016 PCrLJ 1790
Nawad alias Nawabi vs. The State, 1985 PCrLJ 2217
Packages Limited vs. Muhammad Maqbool & others, PLD 1991 SC 258
Qari Kafait Ullah vs. The State, 2008 YLR 1503
Qari Muhammad Ishaq Ghazi vs. The State, 2019 SCMR 1646
Rafi Ullah vs. The State, 2019 PCr.LJ 1608
Raja Waheen Mehfooz vs. Special Judge, ATC-II, Rawalpindi, 2016 PCr.LJ 1773
Raza Munir vs. Mst. Sardar Bibi, 2005 SCMR 1315
Sahib Dino Alias Saboo vs. the State, 2004 PCr.LJ 1765
Salman Alias Lamba and Another vs. The State, 2018 YLR 1092 KHC
Sikandar Ali Lahsari vs. The State, 2016 YLR 62
Sikandar Zulqarnain vs. Habib Bank LTD., PLD 2016 KHC 139
State vs. Sarmad Liaquat; Crl. Misc. No. 69371-B/2017
Subhanuddin vs. State, 1976 SCMR 506
Syed Mushahid Shah & others vs. F.I.A & others, 2017 SCMR 1218
Tahir Ahmed Naseem vs. The State, 2019 YLR 721
Taimoor Mirza vs. Maliha Hussain, 2020 CLC 1029
Tanveer Ahmed vs. The State, 2011 PCr.LJ 677 Karachi High Court
Tanveer Ahmed vs. The State, 2011 PCr.LJ 677 KHC
The State vs. Abdul Qayum, 2001 SCMR 14
The State vs. Raeesuddin Mama S/o Ameenuddin
‘The State vs. Usman Sohail Butt’, DRF 2019

STATUTES

Anti-Money Laundering Act, 2010
Anti-Terrorism Act, 1997
Banker’s Books Evidence Act, 1891
Banking Companies Ordinance, 1962
Capital Development Authority Ordinance, 1960
Central Depositories Act, 1997
Control of Narcotic Substances Act, 1997
Code of Criminal Procedure, 1898
Companies Act, 2017
Customs Act, 1969
Federal Investigation Agency Act, 1974
Foreign Assets (Declaration & Repatriation) Ordinance, 2018
Investigation for Fair Trial Act, 2013
Income Tax Ordinance, 2001
Karachi Development Authority (Revival and Amending) Act, 2016
Lahore Development Authority Act, 1975
Mutual Legal Assistance (Criminal Matters) Act, 2020
NAB Ordinance, 1999
Pakistan Penal Code, 1860
Prevention of Electronic Crimes Act, 2016
Qanun-e-Shahadat Order, 1984
Right of Access to Information Act, 2017
The Securities and Exchange Commission Act, 1997
The Anti-Narcotics Force Act, 1997
The State Bank of Pakistan Act, 1956
Trust Act, 1882
Voluntary Declaration of Domestic Assets Ordinance, 2018
OTHER AUTHORITIES
Black’s Law Dictionary
Investigating Money Laundering and Terrorist Financing
Financial Investigations and Confiscation of Proceeds of Crime: Training Manual for Law
Module 4 - Planning Investigations: Investigation of Corruption and Money
The Role of Hawala and Other Similar Service Providers in Money Laundering And Terrorist Financing
Guide for the Effective Investigation and Prosecution of Money Laundering and Terrorist Financing in Pakistan (“CTF Guide”)

RULES
FBR AML and CFT Regulations for DNFBPs, 2020
Lahore High Court Rules and Order Volume III
Police Rules 1934

TREATISES
International Convention for the Suppression of the Financing of Terrorism (ICSFT)
The Commonwealth Scheme for Mutual Assistance in Criminal Matters (Harare Scheme)
The United Nations Convention against Transnational Organized Crime (UNTOC)

REGULATIONS
SECP Guidelines on Anti-Money Laundering, Countering Financing of Terrorism, and Proliferation Financing, 2020
Anti-Money Laundering, Combating the Financing of Terrorism, & Countering Proliferation Financing (AML/CFT/CPF) Regulations for State Bank of Pakistan’s Regulated Entities, 2020
Pakistan Post (AML and CFT) Regulations, 2020 (S.R.O No. 949(i)/2020
Anti-Money Laundering and Combating Financing of Terrorism Regulations for Cost and Management Accountants and Reporting Firms, 2020
Regulation 30, FATF
SR0 924(1)/2020, FBR
NACTA Standard Operating Procedures for Joint Investigation Team (JIT) for Terrorist Financing Investigations 2020
### TABLE OF ACRONYMS

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>AML/CFT</td>
<td>Anti-Money Laundering/ Counter Terrorism Financing</td>
</tr>
<tr>
<td>AMLA</td>
<td>Anti-Money Laundering Act, 2010</td>
</tr>
<tr>
<td>ANF</td>
<td>Anti-Narcotics Force</td>
</tr>
<tr>
<td>ATA</td>
<td>Anti-Terrorism Act, 1997</td>
</tr>
<tr>
<td>ATC</td>
<td>Anti-Terrorism Court</td>
</tr>
<tr>
<td>CDR</td>
<td>Call Data Record</td>
</tr>
<tr>
<td>CDA</td>
<td>Capital Development Authority</td>
</tr>
<tr>
<td>CTR</td>
<td>Cash Transaction Report</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed-Circuit Television</td>
</tr>
<tr>
<td>CrPC.</td>
<td>Code of Criminal Procedure, 1898</td>
</tr>
<tr>
<td>CNIC</td>
<td>Computerized National Identity Card</td>
</tr>
<tr>
<td>CNSA</td>
<td>Control of Narcotic Substances Act</td>
</tr>
<tr>
<td>CTDs</td>
<td>Counter Terrorism Departments</td>
</tr>
<tr>
<td>CTW</td>
<td>Counter Terrorism Wing</td>
</tr>
<tr>
<td>CDD</td>
<td>Customer Due Diligence</td>
</tr>
<tr>
<td>DNFBP</td>
<td>Designated Non-Financial Businesses and Professions</td>
</tr>
<tr>
<td>DSP</td>
<td>District Superintendent of Police</td>
</tr>
<tr>
<td>e-CIB</td>
<td>Electronic Credit Investigation Bureau</td>
</tr>
<tr>
<td>FBR-IR</td>
<td>Federal Bureau of Revenue – Inland Revenue</td>
</tr>
<tr>
<td>FBR</td>
<td>Federal Bureau of Revenue</td>
</tr>
<tr>
<td>FIA</td>
<td>Federal Investigation Agency</td>
</tr>
<tr>
<td>FATF</td>
<td>Financial Action Task Force</td>
</tr>
<tr>
<td>FI</td>
<td>financial intelligence</td>
</tr>
<tr>
<td>FMU</td>
<td>Financial Monitoring Unit</td>
</tr>
<tr>
<td>FIR</td>
<td>First Information Report</td>
</tr>
<tr>
<td>HDD</td>
<td>Hard Disk Drive</td>
</tr>
<tr>
<td>ITO</td>
<td>Income Tax Ordinance, 2001</td>
</tr>
<tr>
<td>IBMS</td>
<td>Integrated Border Management System</td>
</tr>
<tr>
<td>IBAN</td>
<td>International Banking Account Numbers</td>
</tr>
<tr>
<td>ICSFT</td>
<td>International Convention for the Suppression of the Financing of Terrorism</td>
</tr>
<tr>
<td>IMEI</td>
<td>International Mobile Equipment Identity</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IPDR</td>
<td>Internet Protocol Detail Record</td>
</tr>
<tr>
<td>IFTA</td>
<td>Investigation for Fair Trial Act, 2013</td>
</tr>
<tr>
<td>IO</td>
<td>Investigation Officer</td>
</tr>
<tr>
<td>Acronym</td>
<td>Full Form</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>JIT</td>
<td>Joint Investigation Team</td>
</tr>
<tr>
<td>KDA</td>
<td>Karachi Development Authority</td>
</tr>
<tr>
<td>KYC</td>
<td>Know Your Customer</td>
</tr>
<tr>
<td>LDA</td>
<td>Land Development Authority</td>
</tr>
<tr>
<td>LEA</td>
<td>Law Enforcement Agencies</td>
</tr>
<tr>
<td>LC</td>
<td>Letter of Credit</td>
</tr>
<tr>
<td>MIS</td>
<td>Management Information System</td>
</tr>
<tr>
<td>MoU</td>
<td>Memorandum of understanding</td>
</tr>
<tr>
<td>MoI</td>
<td>Ministry of Interior</td>
</tr>
<tr>
<td>MLA</td>
<td>Mutual Legal Assistance (Criminal Matters) Act, 2020</td>
</tr>
<tr>
<td>MLAR</td>
<td>Mutual Legal Assistance Request</td>
</tr>
<tr>
<td>NAB</td>
<td>National Accountability Bureau</td>
</tr>
<tr>
<td>NAO</td>
<td>National Accountability Bureau Ordinance</td>
</tr>
<tr>
<td>NACTA</td>
<td>National Counter Terrorism Authority</td>
</tr>
<tr>
<td>NADRA</td>
<td>National Database &amp; Registration Authority</td>
</tr>
<tr>
<td>NGO</td>
<td>Non-governmental Organization</td>
</tr>
<tr>
<td>NPO</td>
<td>Non-Profit Organization</td>
</tr>
<tr>
<td>PPC</td>
<td>Pakistan Penal Code</td>
</tr>
<tr>
<td>PTCL</td>
<td>Pakistan Telecommunication Limited</td>
</tr>
<tr>
<td>PECA</td>
<td>Prevention of Electronic Crimes Act, 2016,</td>
</tr>
<tr>
<td>QSO</td>
<td>Qanun-e-Shahadat Order, 1984</td>
</tr>
<tr>
<td>QCR</td>
<td>Quality Control Review</td>
</tr>
<tr>
<td>RIA</td>
<td>Right of Access to Information Act, 2017</td>
</tr>
<tr>
<td>SECP</td>
<td>Securities and Exchange Commission Pakistan</td>
</tr>
<tr>
<td>SBP</td>
<td>State Bank of Pakistan</td>
</tr>
<tr>
<td>SIM</td>
<td>Subscriber Identity Module</td>
</tr>
<tr>
<td>SP</td>
<td>Superintendent of Police</td>
</tr>
<tr>
<td>STR</td>
<td>Suspicious Transaction Reports</td>
</tr>
<tr>
<td>TF</td>
<td>Terrorism Financing</td>
</tr>
<tr>
<td>u/s</td>
<td>Under Section</td>
</tr>
<tr>
<td>UNTOC</td>
<td>United Nations Convention against Transnational Organized Crime</td>
</tr>
<tr>
<td>WeBOC</td>
<td>Web-Based One Customs</td>
</tr>
</tbody>
</table>
GENERAL EVIDENCE KEY
**GENERAL EVIDENCE KEY**

This key provides the Guidelines Code and corresponding Annexure for each type of evidence. The Guidelines Code is used later in this Volume, along with detailed guidelines for each type of evidence, including its evidentiary value and relevancy/admissibility, as well as guidelines for Investigating Officers to collect and analyze that evidence. The Annexures, located at the end of this Volume, include templates for requesting and recording information obtained from each corresponding type of evidence.

<table>
<thead>
<tr>
<th>TYPE OF EVIDENCE</th>
<th>CODE FOR GUIDELINES</th>
<th>ANNEXURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confessional Statement</td>
<td>Code A</td>
<td>–</td>
</tr>
<tr>
<td>Prosecution Witness Statements</td>
<td>Code B</td>
<td>I</td>
</tr>
<tr>
<td>Financial Record</td>
<td>Code C</td>
<td>II</td>
</tr>
<tr>
<td>ːBank Record</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ːBank Locker Record</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ːIncome Tax Returns</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ːWealth Statements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ːRecord of Immoveable Properties</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ːBranchless Banking Records</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ːExcise Department Records</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ːNPO Registration Authority Records</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ːDNFBPs Record</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ːNational Savings etc.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal Profiling Record:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ːVerisys and Family Tree - NADRA,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ːPassport Record - Directorate General of Immigration and Passports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ːGround Verification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ːTravel History Record from FIA IBMS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expert Analysis and Findings</td>
<td>Code D</td>
<td>III</td>
</tr>
<tr>
<td>ːInterception and Surveillance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ːDigital/Cyber Evidence</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ːDigital Equipment like Computer and Mobile Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ːCall Detail Record (CDR) and SIM Registration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ːRecord from Social Media Companies/Apps</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ːAudio Video Recording</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ːDigital Forensics and Evidence</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ːForensics: Fingerprints and Handwriting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Additional Evidence Concerning Relationship with Proscribed Organizations</td>
<td>Code E</td>
<td>–</td>
</tr>
<tr>
<td>ːPamphlets</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ːReceipt Books</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ːWriting Instruments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ːLoudspeakers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ːSkin Hides, etc. (Collection of Donations)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
MONEY LAUNDERING AND TERRORISM FINANCING OFFENCES
IN THIS SECTION

1. Fund Raising (Section 11-H, Anti-Terrorism Act, 1997)
   a. Text of the Provision
   b. Ingredients of the Offence
   c. List of Relevant Evidence
   25

2. Use and Possession (Section 11-I, Anti-Terrorism Act, 1997)
   a. Text of the Provision
   b. Ingredients of the Offence
   c. List of Relevant Evidence
   28

3. Funding Arrangements (Section 11-J, Anti-Terrorism Act, 1997)
   a. Text of the Provision
   b. Ingredients of the Offence
   c. List of Relevant Evidence
   30

4. Money Laundering (Section 11-K, Anti-Terrorism Act, 1997)
   a. Text of the Provision
   b. Ingredients of the Offence
   c. List of Relevant Evidence
   32

5. Support to Proscribed Organizations (Section 11-F(5), Anti-Terrorism Act, 1997)
   a. Text of the Provision
   b. Ingredients of the Offence
   c. List of Relevant Evidence
   34

6. Violation of UN Security Council Resolutions (Section 11-OOO, Anti-Terrorism Act, 1997)
   a. Text of the Provision
   b. Ingredients of the Offence
   c. List of Relevant Evidence
   35

7. Offence of Money Laundering (Section 3, AMLA)
   a. Text of the Provision
   b. Ingredients of the Offence
   c. Predicate Offences
   d. List of Relevant Evidence
   38
1. Fund Raising (Section 11-H, Anti-Terrorism Act, 1997)

a. Text of the Provision

ANTI-TERRORISM ACT, 1997
Section 11-H: Fund Raising
(1) A person commits and offence if he: -
   (a) invites another to provide money or other property; and
   (b) intends that it should be used, or has reasonable cause to suspect that it may be used, for the purposes of terrorism [or by a terrorist or organization concerned in terrorism.]

(2) A person commits an offence if: -
   (a) he receives money or other property; and
   (b) intends that it should be used, or has reasonable cause to suspect that it may be used, for the purposes of terrorism [or by a terrorist or organization concerned in terrorism.]

(3) A person commits an offence if he: -
   (a) provides money or other property; and
   (b) knows or has reasonable cause to suspect that it may or will be used for the purposes of terrorism [or by a terrorist or organization concerned in terrorism.]

(4) In this section a reference to the provision of money or other property is a reference to its being given, lent or otherwise made available, whether or not for consideration.
b. Ingredients of the Offence

<table>
<thead>
<tr>
<th>INGREDIENTS</th>
<th>ACTUS REUS</th>
<th>MENS REA</th>
</tr>
</thead>
<tbody>
<tr>
<td>11-H (1): Invitation to provide money or property for terrorism</td>
<td>Invitation (through any mode e.g. loud speaker, public/crowd addressing, using cyber space, writing request letters etc.) by a person to provide money or other property. Words used for invitation must contain asking/requesting for finances (moveable/immoveable), description of purpose, and the name of the organization/NGO. (An activity for the generation of funds).</td>
<td>With an intention that the money or other property should be used or has a reasonable cause to suspect that it may be used for the purposes of terrorism or by a terrorist or organization concerned in terrorism.</td>
</tr>
<tr>
<td>11-H (2): Receipt of money or other property for terrorism</td>
<td>Receives money or other property (possesses property received as a result of invitation, issues receipts/acknowledgement etc.)</td>
<td>With an intention that the money or other property should be used or has a reasonable cause to suspect that it may be used for the purposes of terrorism or by a terrorist or organization concerned in terrorism.</td>
</tr>
<tr>
<td>11-H (3): Provision of money or other property for terrorism</td>
<td>Provides money or other property (the second-hand of the transaction; the person who provides property to inviter)</td>
<td>With knowledge or reasonable suspicion that it will or may be used for the purposes of terrorism or by a terrorist or organization concerned in terrorism.</td>
</tr>
</tbody>
</table>

---

2 See ATA's section 2 (pa) "person" means any natural, legal person or body corporate.
3 See ATA's section 2 (oa) "money" includes coins or notes in any currency, postal orders, money orders, bank credits, bank accounts, letter of credit, travelers cheques, bank cheques, bankers draft, in any form, electronic, digital or otherwise and such others kinds of monetary instruments or documents as the Federal Government may by order specify.
4 See ATA's section 2 (paa) "property" means property of every description, whether corporeal or incorporeal, movable or immovable, tangible or intangible and includes shares, securities, bonds and deeds and instruments evidencing title to, or an interest in, property of any kind and money.
5 The term reasonable cause to suspect has not been defined in the Anti-Terrorism Act, 1997. However, it has been explained by the Supreme Court of the United Kingdom in R v. Sally Lane and John Letts [2018 UKSC 36] that it is an objective assessment to be made based on the facts and circumstances of each case. The test is that would a reasonable person in the accused's position – based on the information he possess – have a reason to suspect that the money or other property would or may be used for the purpose of terrorism. The Supreme Court of the UK observed, "the requirement of an objectively assessed cause for suspicion focuses attention on what information the accused had. The requirement is satisfied when, on the information available to the accused, a reasonable person would suspect that the money might be used for terrorism."

Since this is an objective test, it is not necessary to prove that the accused actually suspected that the money or other property may be used for terrorism but rather that a reasonable person with the same knowledge would so suspect.

6 See ATA's section 11A Organization concerned in terrorism. - (1) For the purposes of this Act, an organization is concerned in terrorism if it –
(a) Commits (facilitates) or participates in acts of terrorism;
(b) Prepares for terrorism;
(c) Promotes or encourages terrorism;
(d) Supports and assists any organization concerned with terrorism;
(e) Patronizes and assists in the incitement of hatred and contempt on religious, sectarian or ethnic lines that stir up disorder;
(f) Fails to expel from its ranks or ostracize those who commit acts of terrorism and presents them as heroic persons; or
(g) Is otherwise concerned in terrorism.

(2) An organization shall fall within the meaning of sub-section (1) if it–
(a) Is owned or controlled, directly or indirectly, by a terrorist or an organization referred in sub-section (1), or
(b) Acts on behalf of, or at the direction of, a terrorist or an organization referred in sub-section (1).
c. List of Relevant Evidence

<table>
<thead>
<tr>
<th>TYPE OF EVIDENCE</th>
<th>CODE FOR GUIDELINES</th>
<th>ELEMENTS</th>
<th>CODE FOR GUIDELINES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confessional Statement</td>
<td>11-H(1), 11-H(2), 11-H(3)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Prosecution Witness Statements</td>
<td>11-H(1), 11-H(2), 11-H(3)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Financial Record</td>
<td>11-H(2), 11-H(3)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>* Bank Record</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* Bank Locker Record</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* Income Tax Returns</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* Wealth Statements</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* Record of Immoveable Properties</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* Branchless Banking Records</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* Excise Department Records</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* NPO Registration Authority Records</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* DNFBPs Record</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* National Savings etc.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal Profiling Record:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* Verisys and Family Tree - NADRA,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* Passport Record - Directorate General of Immigration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>and Passports</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* Ground Verification</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* Travel History Record from FIA IBMS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expert Analysis and Findings</td>
<td>11-H(1), 11-H(2), 11-H(3)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>* Interception and Surveillance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* Digital/Cyber Evidence</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Digital Equipment like Computer and Mobile Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Call Detail Record (CDR) and SIM Registration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Record from Social Media Companies/Apps</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ Audio Video Recording</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* Digital Forensics and Evidence</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* Forensics: Fingerprints and Handwriting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Additional Evidence Concerning Relationship with</td>
<td>11-H(1), 11-H(2), 11-H(3)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Proscribed Organizations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* Pamphlets</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* Receipt Books</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* Writing Instruments</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* Loudspeakers</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>* Skin Hides, etc. (Collection of Donations)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2. **Use and Possession (Section 11-I, Anti-Terrorism Act, 1997)**

a. **Text of the Provision**

**ANTI-TERRORISM ACT, 1997**

Section 11-I: **Use and Possession**

A person commits an offence if:

1. he uses money or other property for the purposes of terrorism; or
2. he:
   a. possesses money or other property; and
   b. intends that it should be used, or has reasonable cause to suspect that it may be used, for the purposes of terrorism.

b. **Ingredients of the Offence**

<table>
<thead>
<tr>
<th>INGREDIENTS</th>
<th>ACTUS REUS</th>
<th>MENS REA</th>
</tr>
</thead>
<tbody>
<tr>
<td>11-I (1): - Use of money or other property for terrorism</td>
<td>Use of money or other property. The uses of money can be terrorism/terrorist operations, propagation of ideology, recruitment, training, procurements, managing organizational infrastructure, social services to members etc.</td>
<td>For the purposes of terrorism.</td>
</tr>
<tr>
<td>11-I (2): - Possession of money or other property for terrorism</td>
<td>Possesses money or other property. This includes management of funds in the form of bank accounts, real estate, cash in boxes, gems and minerals, jewelry, front businesses, front NPOs, etc.</td>
<td>With an intention that the money or other property should be used, or has reasonable cause to suspect that it may be used for the purposes of terrorism.</td>
</tr>
</tbody>
</table>

c. **List of Relevant Evidence**

<table>
<thead>
<tr>
<th>TYPE OF EVIDENCE</th>
<th>ELEMENTS</th>
<th>CODE FOR GUIDELINES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confessional Statement</td>
<td>✔️ ✔️</td>
<td>A</td>
</tr>
<tr>
<td>Prosecution Witness Statements</td>
<td>✔️ ✔️</td>
<td>B</td>
</tr>
</tbody>
</table>
### Financial Record
- Bank Record
- Bank Locker Record
- Income Tax Returns
- Wealth Statements
- Record of Immoveable Properties
- Branchless Banking Records
- Excise Department Records
- NPO Registration Authority Records
- DNFBP's Record
- National Savings etc.

### Personal Profiling Record:
- Verisys and Family Tree - NADRA,
- Passport Record - Directorate General of Immigration and Passports
- Ground Verification
- Travel History Record from FIA IBMS

### Expert Analysis and Findings
- Interception and Surveillance
- Digital/Cyber Evidence
  - Digital Equipment like Computer and Mobile Data
    - Call Detail Record (CDR) and SIM Registration
    - Record from Social Media Companies/Apps
  - Audio Video Recording
- Digital Forensics and Evidence
- Forensics: Fingerprints and Handwriting

### Additional Evidence Concerning Relationship with Proscribed Organizations
- Pamphlets
- Receipt Books
- Writing Instruments
- Loudspeakers
- Skin Hides, etc. (Collection of Donations)

---

### 3. Funding Arrangements (Section 11-J, Anti-Terrorism Act, 1997)

#### a. Text of the Provision

**ANTI-TERRORISM ACT, 1997**

**Section 11-J. Funding Arrangements**

1. A person commits an offence if he:
   - (a) enters into or become concerned in an arrangement as a result of which money or other property is made available or is to be made available to another; and
   - (b) has reasonable cause to suspect that it will or may be used for the purposes of terrorism.

2. Any person in Pakistan or a Pakistani national outside Pakistan shall commit an offence under this Act, if he knowingly or willfully makes money or other property or services available, directly or indirectly, wholly or jointly, for the benefit of a proscribed organization or proscribed person.
(3) A person commits an offence if he knowingly or willfully pays for or provides money or other property or facilitate in any manner the travel of a person anywhere for the purposes of perpetrating, participating in, assisting or preparing for a terrorist act or for the purpose of providing or receiving training for terrorist related activities.

(4) The provisions of sub-section (2) shall also apply to-
   (a) organizations owned or controlled, directly or indirectly, by proscribed organizations or proscribed persons;
   and
   (b) persons or organizations acting on behalf of, or at the direction of, proscribed organizations or proscribed persons.

b. Ingredients of the Offence

<table>
<thead>
<tr>
<th>INGREDIENTS</th>
<th>ACTUS REUS</th>
<th>MENS REA</th>
</tr>
</thead>
<tbody>
<tr>
<td>11-J (1): - Entering into an arrangement for provision of money or other property for terrorism</td>
<td>Entering or becoming concerned in an arrangement as a result of which money or other property is made available or is to be made available to another. This includes front businesses, NPOs, illegal MVTS, cash smuggling, bank accounts etc.</td>
<td>With a reasonable cause to suspect that money or other property will or may be used for terrorism.</td>
</tr>
<tr>
<td>11-J (2): - Assistance/ provision of money or other property or services to proscribed persons or organizations, organizations owned or controlled directly or indirectly by proscribed persons and organizations, and persons or organizations acting on behalf of or at the direction of proscribed persons or organizations</td>
<td>Knowingly or willfully makes money or other property or services available, directly or indirectly, wholly or jointly, for the benefit of a proscribed organization or proscribed person. This includes associates, front-men, front NPOs.</td>
<td>Willfully and with knowledge.</td>
</tr>
<tr>
<td>11-J (3): - Provision of money or other property or facilitation of travel for the purposes of terrorism</td>
<td>Knowingly or willfully pays for or provides money or other property or facilitates in any manner the travel of a person anywhere for the purposes of perpetrating, participating in, assisting or preparing for a terrorist act or for the purpose of providing or receiving training for terrorist related activities. (One of the uses of terrorist activity)</td>
<td>Willfully and with knowledge.</td>
</tr>
</tbody>
</table>
### List of Relevant Evidence

<table>
<thead>
<tr>
<th>TYPE OF EVIDENCE</th>
<th>ELEMENTS</th>
<th>CODE FOR GUIDELINES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Actus Re</td>
<td>Mens Rea</td>
</tr>
<tr>
<td>Confessional Statement</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Prosecution Witness Statements</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Financial Record</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Bank Record</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>• Bank Locker Record</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>• Income Tax Returns</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>• Wealth Statements</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>• Record of Immoveable Properties</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>• Branchless Banking Records</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>• Excise Department Records</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>• NPO Registration Authority Records</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>• DNFBPs Record</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>• National Savings etc.</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Personal Profiling Record:</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>• Verisys and Family Tree - NADRA,</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>• Passport Record - Directorate General of Immigration and Passports</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>• Ground Verification</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>• Travel History Record from FIA IBMS</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Expert Analysis and Findings</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>• Interception and Surveillance</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>• Digital/Cyber Evidence</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>• Digital Equipment like Computer and Mobile Data</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>• Call Detail Record (CDR) and SIM Registration</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>• Record from Social Media Companies/Apps</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>• Audio Video Recording</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>• Digital Forensics and Evidence</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>• Forensics: Fingerprints and Handwriting</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Additional Evidence Concerning Relationship with Proscribed Organizations</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>• Pamphlets</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>• Receipt Books</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>• Writing Instruments</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>• Loundspeakers</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>• Skin Hides, etc. (Collection of Donations)</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
4. **Money Laundering (Section 11-K, Anti-Terrorism Act, 1997)**

a. **Text of the Provision**

**ANTI-TERRORISM ACT, 1997**

*Section 11-K. Money Laundering:*

(1) A person commits an offence if he enters into or becomes concerned in any arrangement which facilitates the retention or control, by or on behalf of another person, of terrorist property: -

(a) By concealment;
(b) By removal from the jurisdiction;
(c) By transfer to nominees; or
(d) In any other way.

(2) It is a defense for a person charged with an offence under sub-section (1) to prove that he did not know and had no reasonable cause to suspect that the arrangement related to terrorist property.

b. **Ingredients of the Offence**

<table>
<thead>
<tr>
<th>INGREDIENTS</th>
<th>ACTUS REUS</th>
<th>MENS REA</th>
</tr>
</thead>
<tbody>
<tr>
<td>11-K- Money Laundering</td>
<td>Entering into or becoming concerned in an arrangement which facilitates the retention or control of terrorist property by concealment, removal from jurisdiction, transfer to nominees or in any other manner.</td>
<td>If the accused proves that he did not know, or had no reasonable cause to suspect that the arrangement related to terrorist property, that is a valid defense. The onus to prove this would lie with the accused.</td>
</tr>
</tbody>
</table>

This includes front-men, front-businesses, front NPOs, DNFBPs, illegal MVTS, cash smuggling etc.

c. **List of Relevant Evidence**

<table>
<thead>
<tr>
<th>TYPE OF EVIDENCE</th>
<th>ELEMENTS</th>
<th>CODE FOR GUIDELINES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confessional Statement</td>
<td>✔️</td>
<td>A</td>
</tr>
<tr>
<td>Prosecution Witness Statements</td>
<td>✔️</td>
<td>B</td>
</tr>
<tr>
<td>Financial Record</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Bank Record</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Bank Locker Record</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Income Tax Returns</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Wealth Statements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Record of Immoveable Properties</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Branchless Banking Records</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Expert Analysis and Findings
• Interception and Surveillance
  • Digital/Cyber Evidence
    ■ Digital Equipment like Computer and Mobile Data
      - Call Detail Record (CDR) and SIM Registration
      - Record from Social Media Companies/Apps
    ■ Audio Video Recording
  • Digital Forensics and Evidence
  • Forensics: Fingerprints and Handwriting

Personal Profiling Record:
• Verisys and Family Tree - NADRA,
• Passport Record - Directorate General of Immigration and Passports
• Ground Verification
• Travel History Record from FIA IBMS

Additional Evidence Concerning Relationship with Proscribed Organizations
• Pamphlets
• Receipt Books
• Writing Instruments
• Loudspeakers
• Skin Hides, etc. (Collection of Donations)

5. Support to Proscribed Organizations (Section 11-F(5), Anti-Terrorism Act, 1997)

a. Text of the Provision

ANTI-TERRORISM ACT, 1997
Section 11-F(5). Membership, Support and Meetings Relating to a Proscribed Organization –
(5) A person commits an offence if he solicits, collects or raises [money or other property] for a proscribed organization.

b. Ingredients of the Offence

<table>
<thead>
<tr>
<th>INGREDIENTS</th>
<th>ACTUS REUS</th>
<th>MENS REA</th>
</tr>
</thead>
<tbody>
<tr>
<td>11-F (5): Soliciting, Collecting or Raising Money or other Property for a Proscribed Organization.</td>
<td>Conducting the act of either soliciting or collecting or raising either money or property for a proscribed organization.</td>
<td>An accused can be held guilty of Section 11F (5) without having any mens rea for the offence. It is a strict liability offence, meaning that the prosecution is not required to establish mens rea on part of the</td>
</tr>
</tbody>
</table>
accused. To secure a conviction, it will be enough for the prosecution to show that the accused committed the actus reus of the offence, regardless of whether he did so intentionally or unintentionally.

c. List of Relevant Evidence

<table>
<thead>
<tr>
<th>TYPE OF EVIDENCE</th>
<th>ELEMENTS</th>
<th>CODE FOR GUIDELINES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Actus Reus</td>
<td>Mens Rea</td>
</tr>
<tr>
<td>Confessional Statement</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Prosecution Witness Statements</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Financial Record</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>• Bank Record</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Bank Locker Record</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Income Tax Returns</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Wealth Statements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Record of Immoveable Properties</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Branchless Banking Records</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Excise Department Records</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• NPO Registration Authority Records</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• DNFBPs Record</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• National Savings etc.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal Profiling Record:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Verisys and Family Tree - NADRA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Passport Record - Directorate General of Immigration and Passports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Ground Verification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Travel History Record from FIA IBMS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Expert Analysis and Findings</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>• Interception and Surveillance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Digital/Cyber Evidence</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Digital Equipment like Computer and Mobile Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Call Detail Record (CDR) and SIM Registration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Record from Social Media Companies/Apps</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Audio Video Recording</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Digital Forensics and Evidence</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Forensics: Fingerprints and Handwriting</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
6. Violation of UN Security Council Resolutions (Section 11-OOO, Anti-Terrorism Act, 1997)

a. Text of the Provision

ANTI-TERRORISM ACT, 1997

11OOO: Violation of UN Security Council Resolution

(1) A person is guilty of an offence if he, in any way whatsoever, refuses or fails to comply with the orders of the Federal Government under section 2 of the United Nations (Security Council) Act, 1948 (XIV of 1948).

(2) A person guilty of an offence under sub-section (1), shall be liable on conviction to imprisonment for a term not exceeding ten years or with fine not exceeding twenty-five million rupees or with both.

(3) If a legal person or body corporate, commits an offence under sub-section (1), such person or body corporate shall be liable on conviction to fine not exceeding fifty million rupees and every director, officer or employee of such legal person or body corporate found guilty of the violation shall be liable on conviction to imprisonment for a term not exceeding ten years or with fine not exceeding twenty-five million rupees or with both.

(4) Notwithstanding anything contained in sub-section (2), of section 11OOO, if any public servant is found negligent in complying with the provisions of sub-section (1), such public servant shall be proceeded again under respective service rules for administrative action.”.

b. Ingredients of the Offence

<table>
<thead>
<tr>
<th>INGREDIENTS</th>
<th>ACTUS REUS</th>
<th>MENS REA</th>
</tr>
</thead>
<tbody>
<tr>
<td>11-OOO: Refusing or failing to comply with the orders of the Federal Government under section 2 of the United Nations (Security Council) Act, 1948 (XIV of 1948).</td>
<td>A person either refusing or failing to comply with the orders of the Federal Government under Section 2 of the UN (Security Council) Act 1948.</td>
<td>An accused person, legal person, or body corporate can be held guilty of Section 11OOO without having any mens rea for the offence. To the extent of private persons (legal or otherwise), Section 11OOO is a strict liability offence, meaning that the prosecution is not required to establish mens rea on part of the accused. To secure a conviction, it will be enough for the prosecution to show that the accused failed to</td>
</tr>
</tbody>
</table>
making and enforcing such provisions in the domestic laws.

A legal person or body corporate either refusing or failing to comply with the orders of the Federal Government under Section 2 of the UN (Security Council) Act 1948.

A public servant being negligent in complying with the orders of the Federal Government under Section 2 of the UN (Security Council) Act, 1948.

To the extent of public servants, Section 11000 can be committed by a public servant if he possesses the mens rea of negligence. The prosecution can establish negligence by showing that the accused public servant failed to observe the standards expected of a public servant in terms of complying with the orders of the Federal Government under section 2 of the United Nations (Security Council) Act, 1948, or similar order.

c. List of Relevant Evidence

<table>
<thead>
<tr>
<th>TYPE OF EVIDENCE</th>
<th>ELEMENTS</th>
<th>CODE FOR GUIDELINES</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Actus Reus</td>
<td>Mens Rea</td>
</tr>
<tr>
<td>Confessional Statement</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Prosecution Witness Statements</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Financial Record</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>- Bank Record</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>- Bank Locker Record</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>- Income Tax Returns</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>- Wealth Statements</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>- Record of Immoveable Properties</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>- Branchless Banking Records</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>- Excise Department Records</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>- NPO Registration Authority Records</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>- DNFBPs Record</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>- National Savings etc.</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Personal Profiling Record:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Verisys and Family Tree - NADRA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Passport Record - Directorate General of Immigration and Passports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Ground Verification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Travel History Record from FIA IBMS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
7. Offence of Money Laundering (Section 3, AMLA)

a. Text of the Provision

ANTI-TERRORISM ACT, 1997
Section 3. Offence of Money Laundering.
A person shall be guilty 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 clause (a), (b) and (c).

Explanation-I. The knowledge, intent or purpose required as an element of an offence set forth in this section may be inferred from factual circumstances in accordance with the Qanun-e-Shahadat Order, 1984.
Explanation-II. For the purposes of proving an offence under this section, the conviction of an accused for the respective predicate offence shall not be required.

b. Ingredients of the Offence

<table>
<thead>
<tr>
<th>INGREDIENTS</th>
<th>ACTUS REUS</th>
<th>MENS REA</th>
</tr>
</thead>
<tbody>
<tr>
<td>S. 3 (a): Acquisition, conversion, possession, use or transfer of property which is proceeds of crime</td>
<td>Acquires, converts, possesses, uses or transfer property 7</td>
<td>With knowledge or having reason to believe that the property is proceeds of crime 8</td>
</tr>
</tbody>
</table>
With knowledge or having reason to believe that the property is proceeds of crime.

With knowledge that an offence under clause (a), (b) or (c) of section 3 has been committed.

Holds or possesses on behalf of any other person any property.

Participates in, associates, conspires to commit, attempts to commit, aids, abets, facilitates or counsel the commission of acts specified in clause (a), (b) & (c) of section 3.

S. 3 (c): - Possession of a property, on behalf of any other person, which is proceeds of crime

S. 3 (d): - Aiding and abetting the offence of money laundering

S. 3 (b): - Concealment of or disguising the true origin or ownership of property which is proceeds of crime

Conceals or disguises the true nature, origin, location, disposition, movement or ownership of property.

With knowledge or having reason to believe that the property is proceeds of crime.

With knowledge that an offence under clause (a), (b) or (c) of section 3 has been committed.

C. Predicate Offences

A predicate offence is the crime through which proceeds of crime are generated and subsequently laundered by placement, layering and integration. The predicate offences to money laundering are included in the 1st Schedule, Anti-Money Laundering Act, 2010.

The following steps constitute the offence:

1. Predicate Offence (generation of proceeds of crime)
2. Placement (introduction of proceeds of crime into the main financial stream)
3. Layering (changing form and location of proceeds of crime with or without intervals of various time-spans to give it a distant look from its origin)
4. Integration (use the proceeds of crime after its laundering / the purpose of ML)

According to the definition provided in Section 3 of AMLA, 2010, every person who is engaged/involved in the process of money laundering, from placement to integration stage, whether he is beneficiary or not and, with knowledge or having reason to believe that the property is proceed of crime, is guilty of the offence.

The following are some of the most common predicate offences:

<table>
<thead>
<tr>
<th>INGREDIENTS</th>
<th>ACTUS REUS</th>
<th>MENS REA</th>
</tr>
</thead>
<tbody>
<tr>
<td>S. 405, Pakistan Penal Code 1860: Criminal Breach of Trust</td>
<td>1) Misappropriation or conversion to one’s own use entrusted property, or property over which dominion is exercised (“Property” or “Trust”); OR</td>
<td>Dishonest intention.(^9)</td>
</tr>
</tbody>
</table>

\(^9\) An accused’s intention is dishonest if, according to the standards of ordinary, honest people, his actions are dishonest.
<table>
<thead>
<tr>
<th>S. 8, The Control of Narcotic Substances Act, 1997 (&quot;CNSA&quot;): Trafficking or Financing of Narcotic Drugs, etc.</th>
<th>Organize, manage, traffic in, or finance the import, transport, manufacturing or trafficking of, narcotic drugs, psychotropic substances or controlled substances, or; Use violence or arms for committing or attempting to commit an offence punishable under the Act.</th>
<th>Dishonest intention.</th>
</tr>
</thead>
<tbody>
<tr>
<td>S. 420, Pakistan Penal Code 1860: Cheating and Dishonestly Inducing Delivery of Property</td>
<td>(1) Cheating to induce victim to deliver any property to any person; OR (2) Cheating to induce victim to make, alter, or destroy whole or part of valuable security; OR (3) Cheating to induce victim to make, alter, or destroy anything which is signed or sealed and is capable of being converted into a valuable security.</td>
<td>Dishonest intention.</td>
</tr>
<tr>
<td>S. 415, Cheating</td>
<td>(1) Deception(^\text{11}) to induce victim to deliver any property to any person; OR (2) Deception to induce victim to give their consent for any other person to retain any property; OR (3) Deception to induce victim to do or omit to do anything which he would not do or omit if he were not so deceived.</td>
<td>Dishonest intention.</td>
</tr>
<tr>
<td></td>
<td>Intention to cause loss to the victim or expose them to a risk of loss.</td>
<td></td>
</tr>
<tr>
<td>Section 8, CNSA is a strict liability offence and, as such, does not require the prosecution to establish mens rea on part of the accused. The mere commission of the actus reus of Section 8 is enough to sustain a conviction.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\(^{10}\) To "dispose of" means to To deal with definitely, to get rid of, to get done with, finish. To make over by way of sale or bargain, sell, 

\(^{11}\) Deception refers to a false representation, made by the accused verbally or through his conduct. A representation is false if the accused knows that the actual state of affairs is different from what he has represented. According to the Explanation to Section 415, a dishonest concealment of facts is deception.
d. List of Relevant Evidence

The following is the list of relevant evidence for Section 3 of the Anti-Money Laundering Act, 2010.

<table>
<thead>
<tr>
<th>TYPE OF EVIDENCE</th>
<th>ELEMENTS</th>
<th>CODE FOR GUIDELINES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confessional Statement</td>
<td>✓ ✓</td>
<td>A</td>
</tr>
<tr>
<td>Prosecution Witness Statements</td>
<td>✓ ✓</td>
<td>B</td>
</tr>
<tr>
<td>Financial Record</td>
<td>✓ ✓</td>
<td>C</td>
</tr>
<tr>
<td>• Bank Record</td>
<td>✓ ✓</td>
<td></td>
</tr>
<tr>
<td>• Bank Locker Record</td>
<td>✓ ✓</td>
<td></td>
</tr>
<tr>
<td>• Income Tax Returns</td>
<td>✓ ✓</td>
<td></td>
</tr>
<tr>
<td>• Wealth Statements</td>
<td>✓ ✓</td>
<td></td>
</tr>
<tr>
<td>• Record of Immoveable Properties</td>
<td>✓ ✓</td>
<td></td>
</tr>
<tr>
<td>• Branchless Banking Records</td>
<td>✓ ✓</td>
<td></td>
</tr>
<tr>
<td>• Excise Department Records</td>
<td>✓ ✓</td>
<td></td>
</tr>
<tr>
<td>• NPO Registration Authority Records</td>
<td>✓ ✓</td>
<td></td>
</tr>
<tr>
<td>• DNFBPs Record</td>
<td>✓ ✓</td>
<td></td>
</tr>
<tr>
<td>• National Savings etc.</td>
<td>✓ ✓</td>
<td></td>
</tr>
<tr>
<td>Personal Profiling Record:</td>
<td>✓ ✓</td>
<td></td>
</tr>
<tr>
<td>• Verisys and Family Tree - NADRA,</td>
<td>✓ ✓</td>
<td></td>
</tr>
<tr>
<td>• Passport Record - Directorate General of Immigration and Passports</td>
<td>✓ ✓</td>
<td></td>
</tr>
<tr>
<td>• Ground Verification</td>
<td>✓ ✓</td>
<td></td>
</tr>
<tr>
<td>• Travel History Record from FIA IBMS</td>
<td>✓ ✓</td>
<td></td>
</tr>
<tr>
<td>Expert Analysis and Findings</td>
<td>✓ ✓</td>
<td>D</td>
</tr>
<tr>
<td>• Interception and Surveillance</td>
<td>✓ ✓</td>
<td></td>
</tr>
<tr>
<td>• Digital/Cyber Evidence</td>
<td>✓ ✓</td>
<td></td>
</tr>
<tr>
<td>• Digital Equipment like Computer and Mobile Data</td>
<td>✓ ✓</td>
<td></td>
</tr>
<tr>
<td>• Call Detail Record (CDR) and SIM Registration</td>
<td>✓ ✓</td>
<td></td>
</tr>
<tr>
<td>• Record from Social Media Companies/Apps</td>
<td>✓ ✓</td>
<td></td>
</tr>
<tr>
<td>• Audio Video Recording</td>
<td>✓ ✓</td>
<td></td>
</tr>
<tr>
<td>• Digital Forensics and Evidence</td>
<td>✓ ✓</td>
<td></td>
</tr>
<tr>
<td>• Forensics: Fingerprints and Handwriting</td>
<td>✓ ✓</td>
<td></td>
</tr>
</tbody>
</table>
INVESTIGATION PROCESS CHARTS AND EXPLANATIONS
IN THIS SECTION

1. Terrorism Financing: Investigation and Prosecution Process Chart
3. Terrorism Financing: Investigation and Prosecution Process Chart Explanation
**TF - Investigation & Prosecution Process Chart**

1. **Information of Offence** → **Intimation to LEA** → **Open of Inquiry**

   - **Team building Investigation + Prosecution**

2. **Registration of FIR**
   - **Statements u/s 161 & Cr.P.C.**
   - **Raid/Searches**
   - **Arrests**
   - **Financial Profiling, Money Trail, Collection of Evidence**
     - **Seize Memos** → **Remand**
     - **Report u/s 173 Cr.P.C.**
     - **Pre Trial Scrutiny**
     - **Trail Farming of Charges**
     - **Conviction, Confiscation, Forfeiture, Acquittal**

3. **Team building Investigation + Prosecution**

   - **Initial of Action**
     - 1. Financial intelligence from FMU
     - 2. Source
     - 3. Intelligence Agencies
     - 4. Referral Mechanisms
     - 5. Open Source
     - Source not to be disclosed

---

- **NADRA**
- **INCOME TAX**
- **BANKS**
- **DIGITAL EVIDENCE**
- **INTELLIGENCE AGENCIES REPORT**
- **SCREENING (PROSCRIBED AND/OR SANCTIONED INDIVIDUALS & ENTITIES,)**
- **PROPERTIES MOVABLE +IMMOVEABLE**
- **EXCISE**
- **NPO RECORDS**
- **DNFBPs**
- **MUTUAL LEGAL ASSISTANCE**
- **INTER-AGENCY COORDINATION**
- **ISPs**
- **OPEN SOURCES**
- **CREDIT REFERENCE AGENCIES**
- **INFORMANTS**
- **MERCHANT SERVICE PROVIDERS**
Terrorism Financing: Investigation and Prosecution Process Chart Explanation

1. Designated Law Enforcement Agencies (LEAs)
In Pakistan, provincial Counter Terrorism Departments (CTDs) and Counter Terrorism Wing (CTW) of Federal Investigation Agency (FIA) are legally mandated under the Anti-Money Laundering Act, 2010 (AMLA) and the Anti-Terrorism Act 1997 (ATA) to conduct investigation of Terrorism Financing (TF) offences. In practice and after designation of CTDs under AMLA-2010, a majority of the TF investigations are conducted by provincial CTDs. However, matters which are of an inter-provincial, transnational or high-profile nature are investigated by FIA CTW at the federal level. In certain cases, joint task forces of CTDs and CTWs also investigate TF cases of a complex nature.

2. Information of an Offence
Prior to any step being undertaken to initiate a criminal investigation or prosecution for a TF offence, information regarding the possible commission of an offence must be generated by an appropriate source. Once such information is communicated to the concerned LEA, the LEA opens an inquiry based on whether it reasonably suspects that an offence has been committed. The following are the common sources of information through which information of a TF offence can arise:

   a. Financial Intelligence
      The Financial Monitoring Unit (FMU) is the concerned department which generates financial intelligence (FI) on the basis of Suspicious Transaction Reports (STRs) / Cash Transaction Report (CTRs) initiated by any financial institution.

   b. Source Information
      Every LEA has source deployment mechanism from where it can have a source report on the basis of which TF investigation can be initiated.

   c. Referral from Intelligence Agencies
      LEAs can also receive a referral report from any intelligence agency of Pakistan on the basis of which a TF investigation can be initiated.

   d. Referral from other LEAs/Regulators/Supervisors
      Any other LEA/Regulator/Supervisor, while conducting its mandated operations comes across the suspicion of the commission of a TF offence, can refer it to CTD or FIA CTW for initiation of TF investigation.

   e. International Request
      If a request of whatsoever nature from a foreign jurisdiction is received through formal or informal channel and the concerned authorities have reasonable cause to believe that it pertains in some way to TF, such authority can refer the matter to CTD or FIA CTW to initiate an TF investigation.

   f. Open-Source Information
      Designated LEAs can initiate TF investigation on any lead found in print, electronic or social media or from any other form of open source available in cyber space.

   g. Financial Informant
      Designated LEAs can initiate TF investigation on the basis of information from financial informants. As a general rule, pseudonymous and anonymous complaints cannot be entertained, however, in matters of terrorism and TF such complaints can be entertained if, after conducting preliminary enquiry, reasonable cause to suspect the commission of a TF offence is found. This exception exists since in most cases of a similar nature the public hesitates in disclosing their identity while filing such complaints.

      LEAs have legal cover under Article 8 of Qanun-e-Shahadat Order, 1984 (QSO) and are not bound to disclose source of information. Similarly, under section 34 of AMLA 2010, LEAs are not bound to disclose their source of information when it is financial intelligence from FMU.

      TF can be identified at any stage of generation, movement, management or use of funds by the proscribed entity/individual directly or through associates/front-men.
3. **Opening an Inquiry**

The preliminary inquiry, prior to registering an FIR, is an important stage in a case. It is important to provide guidelines regarding the purpose of the inquiry and what methods can be used at this stage. This section highlights the purpose and potential methods available. Since the focus is on identifying relevant persons, facts of the offence and charting all entities involved, discreet methods may be more suitable in this regard.

- **Purpose**
  - Figuring out the basic scheme of the TF operation;
  - Identifying the individuals and legal entities involved in the TF operation;
  - Identifying which offences have been committed, TF and otherwise;
  - Deciding which individuals to implicate in the FIR;
  - Gathering sufficient material for drafting FIR;

- **Methods of Inquiry**
  - **Overt Methods**
    - Arrests under S. 11EEE & 11EEE of relevant persons;
    - Summoning records from financial institutions;
  - **Covert Methods**
    - Undercover operations;
    - Surveillance;
    - Intercepting.


4. **Registration of FIR**

If, upon receiving the information and conducting an inquiry, the relevant LEA determines that an offence of TF (or any other cognizable offence) is made out, then it is bound to register a First Information Report (FIR) u/s 154 of the Code of Criminal Procedure, 1898 (Cr.P.C).

Once an FIR is registered, the concerned LEA collects all inculpatory and exculpatory evidence. The information is compiled as a report u/s 173, Cr.P.C, which is then submitted before a Court. The LEA may record findings against or in favour of the accused. The Court then decides based on the evidence available whether to charge the accused; however, at no point is the Court under any obligation to follow the opinion/findings of the police and may decide to try the accused even if the LEA finds him not to be involved in the offence.

5. **Initiation of Investigation**

The National Counter Terrorism Authority Pakistan (NACTA) issued a notification dated 27.03.2020 regarding Standard Operating Procedures for JIT/Investigators for Terrorist Financing Investigations. Relevant excerpts from the notification have been included below.

a. **Constitution of Joint Investigation Team (JIT)**

The JIT may be constituted by the Government in accordance with section 19(1)-ATA. The JIT is headed by investigating officer of Police not below the rank of Superintendent of Police (BS-18) and other officers of JIT may include officers of equivalent rank from intelligence agencies, armed forces and civil armed forces. The JIT comprises of five members and for meeting purposes, the quorum shall be three members. The JIT shall initiate investigation after notification by the Home Department.
b. Investigation Parameters of JIT/Investigating Officers

i. To conduct parallel financial investigations in each terrorism case immediately after its registration, the JIT/investigator shall launch a prompt and parallel financial enquiry; however, the said enquiry shall be within the ambit of the main investigation.

ii. To identify the sources of funding of terrorist activities in accordance to “follow the money” principles, whether small or complex investigations to conduct pro-active TF investigations to detect, prevent terrorist attacks or conduct reactive TF investigations to terrorism events;

iii. To identify the financiers of terrorist activities i.e. donors, fundraisers, facilitators, operatives, or any other person or organisation associated with the terrorist financing activity.

iv. To identify the linkages between origin of the funds or any other property, its intermediaries and ultimate beneficiaries, when the funds or property is used to support terrorism or the financing of terrorism crimes; to use a wide range of investigative techniques suitable for the investigation of terrorist financing and the associated offences. These investigative techniques may include undercover operations, intercepting communications, accessing computer systems and controlled delivery and measures subject to respective laws.

v. To target wide range of TF activity by investigating wide range of cases in line with threats identified in Pakistan’s National Risk Assessment (NRA) and subsequent information made available to LEAs on the TF threats and profiles of terrorist organizations.

vi. To account for the terrorist financing threats/risks/channels identified during the course of investigations conducted including identification of donations including non-profit organizations, charities and sympathisers and proceeds of crime from relating to drug trafficking, kidnapping for ransom, extortion, dacoity/robbery, cash smuggling, environmental crime and TF relating to, proceeds of smuggling-including natural resources, hundi/hawalas, virtual currencies and other methods for transferring of funds used to support terrorism.

vii. JIT/investigator shall adopt effective risk-based procedures to investigate terrorist financing including transnational funding aspect in all TF cases with emphasis on the following:

viii. The transnational TF threat assessment, and transnational threat profiles of terrorist organizations must be made part and parcel of all TF investigations by JITs/investigators.

ix. The transnational (incoming and outgoing) TF aspect must be explored in all TF investigations minutely.

x. The networks involved in transnational funding must be explored, eliminated and brought to justice.

xi. To access the widest possible range of financial, administrative and law enforcement information, including open or public sources such as international reports, guidance documents, typologies, best practices and information collected and/or maintained by other government departments and organizations. This may include information from FMU, SBP, SECP, FIA, ANF, Customs, NADRA, revenue authorities, excise departments, passport & immigration, cellular companies, forensic labs, PTA, social welfare & industries departments, district police.

xii. To identify money or other property owned or controlled, wholly or partly, directly or indirectly, by a proscribed person or organization during the course of investigation for necessary action under 11O of the ATA.

xiii. To identify financial nexus between financing including funding and various techniques used by terrorist organizations to finance terrorist activities.

xiv. To fully investigate use of formal as well as informal means used for identifying the flow / movement of funds to identify, all facilitators (companies/individuals etc.) involved in movement of terrorist funds.

xv. To apply effectively the terrorist financing provisions of the relevant laws for the prosecution and conviction of terrorism financing.

c. Responsibilities of JIT/Investigators/Investigating Officers

i. General

• To examine the crime scene(s) and ensure that an accurate site map is prepared including the cataloguing of evidence seized.
• To examine situation report – first inspection notes.
• To ensure that the offices, business premises, frequently visited places and residences of the accused are thoroughly searched and all records, whether manual or digital, including receipts, diaries, ledgers, computers, discs, USBs etc. are taken into custody through proper seizure protocols in accordance with the policy and procedures.
• To make maximum use of human intelligence throughout the investigation process.
• To identify any witnesses, including house-to-house enquiries.
• To identify and investigate the accused & to find out his previous record.
• To identify any co-suspects in the case.
• To implement an appropriate investigation strategy.
• To implement a forensic management strategy for analysis of evidence collected including securing necessary expertise to examine.
• To ensure proper use of resources that has been allocated to the investigation.
• To seek assistance from FIA, FMU, SECP and SBP for the purposes of conducting of the financial investigations. These agencies may facilitate in analysis of; financial intelligence reported against the suspects, bank statements, complex transactions, linking multiple accounts/transactions with suspects and detecting possible linkage of transactions across different financial channels.
• To seek assistance and cooperation from other federal/provincial departments and state organisations, wherever required.

ii. Terrorist Financing
• To verify that the case is of terror financing, as enumerated in sections 11F(5)(6), 11H to 11K & 11- N of ATA.
• To ensure that members of JIT/investigators are fully briefed by the former IO or complainant & witnesses, where applicable.
• To collect the national identity card (CNIC) number of the accused/associates and check their accounts details, transactions through currency exchange institutions and from companies running branchless banking i.e. Omni, Easy Paisa, and U-Paisa etc. under the applicable laws.
• To contact Money Service Businesses (MSBs) for any possible transactions of the accused.
• To jointly take up the call data records, financial records and personal interviews of the accused person for developing perspective on identification of other key individuals and their financial links with the accused.
• To obtain the details of lockers, which might be maintained by the person, while writing to banks and financial institutions for the account statements. Such lockers will be carefully searched after securing proper court order.
• To use modern financial investigation tools and software as well such as I2, when the scope of financial investigation expands.
• To maintain record of the statements of officers, wherever financial record is obtained from a third party such as banker or Registrar of Companies etc, under section 161 of the Code of Criminal Procedure 1898.
• To seek assistance from high end financial experts and where necessary make use of available mechanisms (bilateral and multilateral) for exchange of information in case where the accused has been found to have made use of front businesses for layering, multiple bank accounts, structuring techniques, dubious charity organizations, shell companies, off shore business structure such as Trusts, etc.
• To find out the facilitator/sympathisers of organizations who make donations to proscribed organizations.
• To affect recovery of the receipts of proscribed organizations from the accused.
• To prepare recovery memo & incorporate the denomination of currency notes and numbers on it.
• To obtain Call Detail Records (CDRs) from telecommunication companies for checking money transactions through cell phones.
To trace out the persons who printed receipts or has made arrangements regarding receipts books.
To find out the communication channel of transactions to proscribed organizations/terrorist networks.
To collect evidence in relation to the case and ensuring preservation by using modern techniques and their despatch for expert examinations.
To manage arrest and interviewing of facilitators, donors and sympathisers of proscribed organizations.
To prepare high quality case files in regular consultation with prosecutors.
To engage with, and utilise the resources of the Intelligence Wing of sister agencies to support the investigative process.
To examine/scrutinize the records as early as possible for developing further lines of investigation and decide immediately as to which of the record or gadgets is to be dispatched for forensic/lab tests.
To keep focus on financial information and the associated non-financial information in the financial documents, such as phone numbers, addresses, passport numbers, etc.
To decide, in consultation with the legal counsel or prosecutor which of the terrorist financing sections of ATA and other laws are attracted, based upon the nature/mode of terrorist financing.
To requisition the video recordings of the CCTV cameras inside or outside the bank and of ATM cameras, to identify the individuals making transactions from the accused or suspects accounts.
To investigate the informal modes of financial transactions made by the targets, associates, nominees used by the suspect(s) from origin to destination including intermediaries to identify the donors, facilitators, beneficiaries and end users in a terrorist activity (Informal modes include Hundi/Hawala, cash couriers or any other mode in the informal sector).
To requisition details of moveable and immoveable assets of individuals and organizations involved in terrorist financing from different agencies including land revenue, housing/development authorities, motor registration authorities etc. (The purpose is to trace the parked assets of terrorists which might be used to facilitate or generate funds for terrorism).

iii. Relevant Recent Amendment to ATA, 1997

Section 19C: Application of investigation techniques. (1) The investigating officer may with the permission of Court, within sixty days of such permission, use techniques including undercover operation, intercepting communications, accessing computer system and controlled delivery for investigation of financing of terrorism under the law in force. The aforementioned period of sixty days may be extended up to further period of sixty days by the Court on a request made to it in writing. The Court may grant extension, if it is satisfied, on the basis of situation or reasons given in the written request. The provisions of this sub-section shall be in addition to and not in derogation of any other law for the time being in force.

6. Conducting Arrest, Remand and Detention of Accused

a. Power of Arrest

A formal arrest authorizes the detention of an individual for a period of twenty-four hours during which the investigation is conducted. Section 46 of the CrPC states that the person making the arrest is to touch and confine the body of the person arrested, unless there is a submission to custody by word or action.

Under the ATA, the police, armed forces and civil armed forces are empowered to arrest an individual without issuing a warrant of arrest. This power of arrest is similar to the provision contained in Section 54 CrPC whereby an officer may arrest a person without a warrant on nine grounds. It is important to note that under Section 54 CrPC, the wide powers of arrest have been limited by requiring the police to make an arrest on the basis of either "credible information" or "reasonable suspicion". Similarly, under Section 5 (2)(ii) of the ATA, a reasonable suspicion that a person has...
committed, or is likely to commit, an act or offence of terrorism has to exist.

Section 60 of CrPC provides that a person arrested without warrant should be produced before a magistrate having requisite jurisdiction without unnecessary delay. Section 61 of the CrPC curtails the powers of a police officer to detain persons arrested for more than twenty-four hours in the absence of a special order from a magistrate under Section 167 of the CrPC.

“Reasonable suspicion” does not mean a vague surmise or inference but rather a bona fide belief on part of the police that an offence has been committed or was about to be committed. Such belief must be founded on some definite averments/allegations that may create the basis for suspicion of the involvement in the offence of the person to be arrested.\(^\text{15}\)

Safeguards in relation to an arrest are laid down in Article 10 of the Constitution of Pakistan, 1973.\(^\text{16}\)

b. Remand and Detention of Accused

Section 21 E of ATA operates in consonance with Section 167 of the CrPC, which comes into force when the investigation cannot be completed within 24 hours. The police may be required to detain the accused in police custody for the purposes of interrogation. The time period may extend to 90 days.

In the judgment, *Raja Waheen Mehfooz v. Special Judge, Anti-Terrorism Court*,\(^\text{17}\) it was held that, the learned Special Court under Anti-Terrorism Act, while dealing with the matters of remand of the accused persons, is equally responsible to observe the provisions of Section 167(3) CrPC.

The ATA has a widely used preventive detention regime. There are two layers of preventive detention:

- The first relates to the detention of a person already proscribed under S. 11EE of the ATA and to the placement on the Fourth Schedule of the ATA subject to the limitations set by Art. 10 of the Constitution of Islamic Republic of Pakistan 1973.
- The second relates to detention for the purposes of inquiry to which Art. 10 of the Constitution of Islamic Republic of Pakistan, 1973 also applies.

The inquiry under Section 11EEE may be conducted by a police officer not below the rank of a Superintendent of

\[\begin{array}{|c|c|c|c|c|c|}
\hline
\text{IMPLEMENTING LAW} & \text{OPERATIVE CLAUSE} & \text{PERIOD OF DETENTION} & \text{DETENTION AUTHORITY} & \text{MECHANISM FOR INITIATING DETENTION} & \text{AIM OF DETENTION} \\
\hline
\text{Anti-Terrorism Act (1997)} & \text{S. 11EEE: arrest and detention of suspected persons} & \text{Initial period of three months} & \text{Federal Government, Armed Forces, Civil Armed Forces} & \text{An order is issued by the Government directing detention and specifying custody and the period of detention} & \text{To prevent persons proscribed under S.11EE ATA from committing offences relating to terrorism, national security and sectarian violence} \\
\hline
\end{array}\]


\(^{16}\) Under Article 10 (2), an individual who is arrested and detained in custody shall be produced before a magistrate within a period of twenty-four hours of such arrest. The Constitution forbids the continued detention of an individual beyond twenty-four hours without the authority of a magistrate.

\(^{17}\) Raja Waheen Mehfooz v. Special Judge, Anti-Terrorism Court-II, Rawalpindi, 2016 PCrLJ 1773.
Police (SP)—or through a JIT read in light with Section 19 of the ATA to be notified by the Government that may include representatives from the police, and civil armed forces and other investigation agencies such as the FIA.\(^\text{18}\)

Provided that where the provisions of sections 4 and 5 have been invoked, the investigation shall be conducted by the JIT comprising of members of armed or civil armed forces, intelligence agencies and other law enforcement agencies, including an investigating officer of police not below the rank of Inspector who shall sign the report under Section 173 of the Code and forward it to the Court.

During this inquiry, the concerned police officer of the Court or any other LEA member of the JIT shall have all the powers of search, arrest, and seizure of property and other belongings of the proscribed individual/organizations as mentioned under the CrPC or any other special law.

Under Section 19(1B) of the ATA, if the person has been arrested by the armed forces, he shall be handed over to the Investigation Officer (IO) of the police station designated by the provincial government.

Under Section 19(5) of the ATA, a person who has been released from police custody under Section 169 of the CrPC or has been remanded to judicial custody, may be subjected to further investigation. An Anti-Terrorism Court (ATC), after recording reasons in writing and upon good grounds shown by a public prosecutor, may order for a person to be placed in police custody or in the custody of the JIT, in order to conduct further investigation in a case. As per Section 19(6), the ATC is considered to be a magistrate for this purpose.

c. Searches under the Anti-Terrorism Act 1997

Sections 165 and 166 of CrPC and Sections 21-B and 19-A of ATA are the relevant provisions governing searches under the Anti-Terrorism Act 1997. An officer in charge of a police station or the police officer making an investigation must ensure that the place being searched is in the correct jurisdiction.

The officer must record, in writing, the grounds for his belief. Section 165 of CrPC empowers the police officer specified to make a search without warrant subject to certain safeguards. The prerequisites for a search as per this section are that:

i. Search must be necessary for investigation;

ii. The offence must be such as the police officer is authorized to investigate, i.e. a cognizable offence;

iii. Reasonable grounds must exist for believing that the thing required will be found in a place;

iv. There would be undue delay in getting the things in any other way;

v. Grounds of belief as to the necessity of search must be previously recorded by the police officer.

These conditions must be fulfilled and there should not be a misuse of the power nor should there be any harassment. The perusal of the section leaves no doubt that it does not apply when search is for arrest of the accused. The search envisaged by this section is to be made for a specified thing. A person is not a thing. ... where police [do] not record in writing in roznamcha (daily diary) grounds for making search of the house of the accused, it was held that it was without jurisdiction and bad in law.\(^\text{19}\)

---

\(^{18}\) The FIA has powers to investigate under Section 5 of the FIA Act, 1974.

\(^{19}\) Muhammad Bilal v. Superintendent of Police, Dera Ghazi Khan, PLD 1999 Lah 297, [8].
Furthermore, as per Rule 25.23 of Police Rules, 1934 an officer in charge of a police station after receiving requisition to search under Section 166 of CrPC should comply without unnecessary delay and should take all necessary precautions to ensure a successful search.

Additionally, under Section 165, if the object in question can be obtained otherwise, the officer is not required to make the search.

Although the provisions of the Cr. P.C. are to apply to searches and arrests made under the ATA, s.19-A of the ATA makes one particular exception: the inapplicability of s.103 of the CrPC. In a nutshell, this provision requires that two or more respectable witnesses of the locality be accompanied by the Police and anything that is taken from the search be signed off by those witnesses. However, under section19-A, the police are under no obligation to take witnesses along for searches.

7. Collection of Financial Record

A financial investigation involves the collection, collation and analysis of all available information with a view towards assisting in the prosecution of crime. The major goal of a financial investigation is to identify and document the movement of money during the course of criminal activity. The link between the origins of the money, beneficiaries, when the money is received and where it is stored or deposited can provide information about and proof of criminal activity.

a. Debriefing Prisoners

Where a terrorist, or terrorism financier is in custody, they may be debriefed with the objective of fully understanding the financing and operations of the terrorist outfit.

b. Credit Reference Agencies (PACRA)

PACRA rating reports may be accessed where information is required regarding the company profiles, ownership structure, governance practices, management practices, risk profile, and financial statements of financial institutions.

c. Directorate of Immigration and Passports

Information can also be obtained from the Directorate of Immigration and Passports that can help in preparing a person’s profile and can identify other lines of enquiry. This includes the following:

- Name
- Gender
- Place of birth
- Addresses
- Passport number
- Names of family members
- Method of payment for passport
- Travel history – Where have they travelled to and how often

[See Guideline Code C and Vol. II of AML/CFT Toolkit for detail.]

8. Inter-Agency Coordination

While collecting evidence, the investigator/JIT must follow the inter-agency coordination mechanism under Multilateral MOU of NACTA. The MOU is between 14 LEAs, including but not limited to the CTDs, FIA, NAB, ANF, FBR, FMU and Intelligence Agencies amongst others.

The objective of this MOU is to enhance interagency coordination and facilitate the timely and effective detention, analysis, and probe of cases, transactions and activities that pertain to AML/CFT. The MOU is also meant to ensure that any such data

---

20 Shahid Hussain v. The State, 2020 MLD 1248 (Lah)
shared amongst organizations would be used only in an authorized fashion with the strictest confidentiality. Any request for information must be provided with a statement of relevant facts, details of new trends, personal information (CNIC etc.) of suspected persons, and details of assets under investigation. In the MOU, it was agreed that LEAs should investigate all predicate crimes from a TF perspective and develop their own SOPs to facilitate such investigations. As a reference, it was recommended that LEAs should consider the SOPs issued by NACTA.

Hence, the FIA’s CTW and provincial CTDs can form a joint investigative team (JIT) to investigate TF cases together. LEAs can obtain information related to ML or a suspicious transaction from the FMU in an investigation, including NAB (section 27 of NAO), ANF (sections 31, 67 and 69 of CNSA) and FBR-IR (section 176 of ITO). However, FBR-Customs FIA has faced challenges in obtaining information held by the FIA.

9. **Expert Analysis and Findings**

[See Guidelines Code D for detail]

10. **Ascertainment of Relevant Sections of Offence to be Charged**

In light of evidence available on record, the investigator/JIT will determine the nature of offence to be charged. Description of the role of each accused must be clearly provided i.e. primary accused, facilitators, associates etc.

11. **Submission of Report u/s 173 CrPC.**

After conclusion of investigation, such report is to be submitted in trial Court along with:

- Facts mentioned in FIR;
- Incriminating evidence in the form of statements u/s 161 and 164 CrPC. 1898 (list of witnesses) and seizure memos (list of documentary / digital evidence / expert opinions);
- Inculpatory and exculpatory evidence;
- Detailed description of role of each accused;
- Description of sections of offences against each accused;
- Prayer to initiate trial.

12. **Trial Stage**

After submission of Report under Section 173 CrPC, the trial commences and follows the below mentioned sequence:

- Before framing of charge, u/s 19B of ATA-1997, the prosecutor is mandated to conduct pre-trial scrutiny of the Report submitted u/s 173 CrPC. 1898.
- Scrutiny of Challan: U/s 173 of the CrPC, the prosecutor can send the report back for removal of evidential weaknesses in case evidential test is not satisfied. If the test is satisfied, then the case moves towards framing of charges.
- Charge is framed
- Trial is initiated
- Conviction and confiscation of assets takes place
- Appeals may be filed
- Finality of order: Either conviction and forfeiture, or acquittal and dismissal of the case.
Money Laundering: Investigation and Prosecution Process
Chart Explanation

1. Designated Law Enforcement Agencies
Under AMLA 2010 following LEAs are designated to conduct investigation of a ML offence:
   - Federal Investigation Agency
   - National Accountability Bureau
   - Counter Terrorism Department
   - Anti-Narcotics Force
   - FBR – Income Tax
   - FBR – Customs Intelligence

[For details, see Guidelines Code C]

2. Initiation of Action
LEAs can initiate ML investigations on the basis of identification of a property (moveable or immoveable), in respect of whom reasonable grounds to suspect exist that it is or is acquired from proceeds of crime, in the following scenarios:

a. Financial Monitoring Unit (FMU)
The FMU, based on a Suspicious Transaction Report (STR) or Currency Transaction Report (CTR) filed by a financial institution, may conduct an inquiry to determine whether the offence of money laundering has been committed. If reasonable suspicion of money laundering having taken place arises, the FMU may forward the information to the concerned LEA, which may lodge an FIR against the accused.23

b. Source Information
Every LEA has source deployment mechanisms from where it can have a source report on the basis of which ML investigation can be initiated.

c. LEA
Generally, the FMU mechanism should be used to trace and weed out money launderers. However, if an LEA has received reliable and credible information of money laundering through its own sources, then it may, on its own motion, open an inquiry, lodge an FIR, and investigate under AMLA, 2010.24

d. Referral from Intelligence Agencies
LEAs can also receive a referral report from any intelligence agency of Pakistan on the basis of which an ML investigation can be initiated.

e. Referral from other LEAs/Regulator/Supervisor
Any other LEA/Regulator/Supervisor, while conducting its mandated operations comes across the possibility of the commission of an ML offence, can refer it to an LEA which has jurisdiction over the predicate offence.

f. International Request
If some request of whatsoever nature is received through formal or informal channel and the concerned authorities have reasonable cause to believe that element of ML is involved, such authority can refer the matter to the concerned LEA.

---

23 Section 6(4)(c), AMLA, 2010.
24 Misbah Karim v. Federation of Pakistan; PLD 2016 Sindh 462.
g. **Open Source**

Designated LEAs can initiate ML investigation on any lead found in print, electronic or social media or from any other form of open source available in cyber space.

h. **Financial Informant**

Designated LEAs can initiate ML investigation on the basis of information from a financial informant. LEAs have legal cover under Article 8 of Qanun-e-Shahadat Order, 1984 and are not bound to disclose source of information. Similarly, under section 34 of AMLA 2010, LEAs are not bound to disclose their source of information when it is financial intelligence from FMU.

Identification of property can be made at any stage of ML i.e. placement, layering or integration.

3. **Registration of FIR**

Upon receiving information into a cognizable offence, designated LEA registers an FIR u/s 154 CrPC. 1898.

4. **Ascertainment of Property Identified**

Particulars of the identified property are collected from concerned authorities and its valuation is conducted.

5. **Investigation Team**

ML investigations are complex and lengthy in nature which require a synchronized and effective investigation. Team members can be from within the organization or a member can be requested from other department who shall not be below the rank of BS-18.

6. **Special Procedure under AMLA 2010**

According to Section 8 of the AMLA, an investigating officer (IO) is empowered to provisionally attach a property. A property can be provisionally attached when the IO reasonably believes the property to be involved in money laundering. An IO can do this based on reports from the concerned investigating or prosecuting agency, by order in writing, or with prior permission of the Court for a period not exceeding one hundred and eighty days from the date of the order. The courts can further grant extensions for up to 180 days.

According to Section 9, Courts can give the opportunity of hearing to those whose properties are under investigation. As part of the investigation, a show-cause notice may be issued to the accused, calling upon them to explain sources of income, earning or assets through which property has been acquired. After that, the court can pass an order confirming the attachment, retention, seizure or as the case may be, release of the property. When the provisional order of attachment has been confirmed the IO shall forthwith take possession of the attached property.

The attachment or retention or seizure of the property will continue while investigations are being conducted. The IO is further required by the court to submit monthly reports of the progress made in the investigation where property has been provisionally attached. Additionally, in every stage of the investigation, the IO is required to submit a report of proceedings to the relevant head of departments within 48 hours of any action.

7. **Investigation Procedure**

ML investigation follows the provisions of CrPC 1898. Additionally, there are certain provisions under the AMLA that specifically pertain to investigation procedures. These include:

- **Section 13: Power of Survey**

  This section empowers the IO to enter any place within the limits of his jurisdiction and authorization and conduct inspections, check or verify any transactions pertaining to proceeds of crime, or to gather any information which may be useful for the investigation. During the survey, the IO can place marks of identification on the records inspected by him, make inventory of the property in question or record any statement from any person present that may be useful for the investigation. The IO is then required to forward a copy of the report based on the survey to the head of the concerned investigating or prosecuting agency.
Section 14: Search and Seizure
This section lays out the powers of search and seizure afforded to the IO with the prior permission of the Court. An IO can conduct search and seizure if there is a reason to believe that the accused has conducted any ML or related activity, is in possession of such property or has any records or documents that will be useful in the investigations. As such, an IO or an authorized subordinate can enter and search any building, place, vessel, vehicle or aircraft where he has reason to suspect that such record or properties are kept and seize any such record or property found as a result of the search. The IO is then required to forward a copy of the report based on the survey to the head of the concerned investigating or prosecuting agency within 48 hours.

Where the investigating officer, upon information obtained during survey under section 13, is satisfied that any evidence shall be or is likely to be concealed or tampered with, he may, for reasons to be recorded in writing, enter and search the building or place where such evidence is located and seize that evidence.

Section 15: Search of Persons
Under this section, an IO is empowered to search any person whom the IO believes has concealed anything pertaining to matters that can be useful to the investigation. According to this section, the IO may search that person and seize such record or property which may be useful for or relevant to any ML proceedings. The IO will further record the statement of the person searched in respect of the records or property involved in money laundering and found or seized in the course of the search. The IO is then required to forward a copy of the report based on the survey to the head of the concerned investigating or prosecuting agency within 48 hours.

8. Collection of Record/Financial Investigation
[See and Vol. II of AML/CFT Toolkit for detail].

9. Establishing the Offence of Money Laundering
The inquiry, investigation, and prosecution of money laundering follows a three-part strategy:

<table>
<thead>
<tr>
<th>PART I</th>
<th>PART II</th>
<th>PART III</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proof of a predicate offence from which illicit wealth is generated (proceeds of crime.)</td>
<td>Proof of money laundering through evidence of financial transactions to conceal or disguise ill-gotten money.</td>
<td>Establishing that the defendant knew that the laundered funds were the proceeds of crime.</td>
</tr>
</tbody>
</table>

PART I: Establishing the Predicate Offence
The predicate offence is a necessary element of money laundering. It is this offence which gives birth to proceeds of crime, the concealment of which attracts the criminal conduct of money laundering. Without the commission of a predicate offence, there can be no conviction for money laundering.²⁵

To establish the predicate offence, the prosecution must gather sufficient facts, information, and materials for a Court to conclude that: (I) the constituent elements of the offence are made out; (II) the defendant is connected to the offences; and (III) a prima facie case against the defendant is made out.

i. Elements of the Offence are fulfilled
Establishing the elements of the offence is a necessary step for gaining a conviction. Unless each element of the offence can clearly be proved against the defendant, gaining a conviction would not be possible.

For the prosecution to establish the elements of the predicate offence, it would be a helpful exercise to carefully study the relevant sections of law under which the defendant is charged for the predicate offence. Each actus reus and mens rea

²⁵ PLD 2021 SC 1.
element of the offence must be identified and separated. This will enable the prosecution to effectively understand the actions, conduct, and accompanying mental state which has been criminalized. Once this is done, it will be far easier for the prosecution and investigating team to identify which facts are relevant and which pieces of evidence useful for establishing their case. Moreover, identifying the elements of the offence can be a useful tool for streamlining the inquiry and investigation.\(^\text{26}\)

Once the *actus reus* and *mens rea* elements have been separated, facts and information gathered during the inquiry and investigation must be arranged such that each element of the offence is established against the defendant. If the facts to establish a certain element are missing, then it must be left to the Court’s discretion to deal with such defect.

**ii. Defendant is connected to the Offences**

The facts must show that the defendant committed the offence, that he actively participated, connived, abetted, or aided the commission of the offence, that he was responsible for it, promoted it, or that he had some stake in it.

**iii. Prima Facie case against Defendant is made out**

Making out a *prima facie* case against the defendant is relevant when it comes to drafting an effective FIR and preventing the defendant from being released in bail. The term “*prima facie*” essentially translates to a ‘case at first sight’. The prosecution must present a *prima facie* case that the Defendant is guilty of the crime charged. It means that when a Court reads the FIR, it must be able to conclude – without having to look at the evidence – that the facts, accusations, and information in the FIR are enough to justify taking the case to trial.

**PART II: Establishing Money Laundering**

Once the predicate offence has been established, the Court should have sufficient information to conclude that the defendant was in possession of proceeds of crime. The next step is to establish money laundering by either detailing the *modus operandi* through which the funds were laundered or presenting evidence of illegal financial transactions.

The rules for establishing the offence of money laundering are the same as for the predicate offence in that the elements of the offence must be fulfilled, the defendant must be connected to the offences, and a *prima facie* case against the defendant must be made out. However, there is the important distinction that the facts pertaining to money laundering will include evidence of illicit financial transactions.

For a transaction to be a part of the money laundering offence, it must be intended to conceal or disguise the true nature, ownership, location, or control of the proceeds of crime.

The following types of financial transactions may be shown to establish money laundering:

<table>
<thead>
<tr>
<th>DOMESTIC TRANSACTIONS</th>
<th>INTERNATIONAL TRANSACTIONS</th>
<th>TRANSACTION OF LARGE AMOUNTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>The types of financial transactions included are deposits, withdrawals, transfers between accounts, exchanges of currency, loans, extensions of credit, purchases or sale of any stock, bonds, certificates of deposit or other monetary instruments, or any other payment, transfer, or delivery by, through, or to a financial institution, by whatever means effected.</td>
<td>International movement of currency, monetary instruments, hundi or hawala transfers, cryptocurrency transactions, or structured transactions.</td>
<td>Evidence of large cash amounts in possession of Defendant, sudden acquisition of extraordinary wealth, or unexplained major expenditures.</td>
</tr>
</tbody>
</table>

\(^{26}\) The investigating team may engage the assistance of a lawyer in identifying the elements of the offence. Additionally, they may use commentaries on criminal laws and case laws to understand the elements of the offence.
Additionally, in establishing money laundering against the defendant, it would be advisable for the prosecution to show that the defendant had no legitimate source of income. This is because the mere possession of any pecuniary resource or property is not an offence, but the defendant's failure to satisfactorily account for such possession of pecuniary resources could constitute an offence.\(^\text{27}\)

The absence of a legitimate source of income can be proved by conducting a net worth analysis of the defendant and identifying whether he has any legitimate sources of income such as employment, self-employment, inheritance, remittance, or other source. Showing that the defendant had no legitimate source of income cements the case against him, proving that his wealth was the proceeds of crime and the financial transactions conducted were to conceal or disguise the true source of income.

**PART III: Establishing that Defendant knew laundered funds were Proceeds of Crime**

As per the plain mandate of Section 3, AMLA 2010, a defendant can only be convicted of money laundering if he knew that the laundered funds were the proceeds of crime.

The prosecution, therefore, must show that the defendant was fully aware and cognizant of the illicit and criminal nature of the source of funds.

i. **Case against Main Defendants**

For the prosecution to establish its case against a main defendant or principal accused who is shown to have committed a predicate offence, there is no need to undertake any separate effort to establish knowledge on part of such a defendant. Since he was the focal person responsible for the predicate offence, it is assumed that he clearly knew that the source of the laundered funds was illegal.

ii. **Case against Abettors**

However, if the prosecution seeks to establish that certain co-accused charged with abetment of money laundering, then it must be separately shown that the abettors were aware that the funds were the proceeds of crime. An abettor may be a legitimate businessperson or professional, such as a property dealer, car dealer, banker, accountant, or lawyer. It is highly likely, but not a certainty, that the businesspersons or professionals were aware that their customer or client's source of income was the proceeds of crime.

In case of such an abettor, knowledge can be established by showing that they profited or benefitted in some way from the predicate offence and money laundering, or by proving that they willfully blinded themselves to the true source of funds by failing to undertake due diligence, by deliberately ignoring the source of funds, or by consciously attempting to avoid knowledge.

iii. **When to Charge an Abettor**

The charge of abetment to money laundering under section 109, PPC should not be brought arbitrarily or whimsically. It should only be brought when the prosecution can show that the abettor: (i) had knowledge of the illegal activity; (ii) had some role in furthering the activity; and (iii) had some stake or derived some benefit from money laundering. Moreover, if the prosecution seeks to implicate an abettor based on financial transactions in favour of the abettor, then the benefit of any transaction must be clearly and visibly established and not be shrouded in mystery.\(^\text{28}\)

10. **Inter-Agency Coordination**

While collecting evidence, the investigator / JIT must follow the inter-agency coordination mechanism under Multilateral MOU of NACTA. The MOU is between 14 LEAs, including but not limited to the CTDs, FIA, NAB, ANF, FBR, FMU and Intelligence Agencies amongst others. The aim is to enhance interagency coordination and facilitate the timely and effective detention, analysis, and probe of cases, transactions and activities that pertain to AML/CFT. The MOU is also meant to ensure that any such data shared amongst organizations would be used only in an authorized fashion with the strictest

\(^{27}\) Maryam Nawaz v. Chairman NAB; PLD 2020 Lah. 205.

\(^{28}\) Maryam Nawaz v. Chairman NAB; PLD 2020 Lah. 205.
confidentiality. Any request for information must be provided with a statement of relevant facts, details of new trends, personal information (CNIC etc.) of suspected persons, and details of assets under investigation. In the MOU, it was agreed that LEAs should investigate all predicate crimes from an ML perspective and develop their own SOPs to facilitate such investigations. LEAs can obtain information related to ML or a suspicious transaction from the FMU in an investigation, including NAB (section 27 of NAO), ANF (sections 31, 67 and 69 of CNSA) and FBR-IR (section 176 of ITO). However, FBR-Customs FIA has faced challenges in obtaining information held by the FIA.
GUIDELINES FOR TYPES OF EVIDENCE
## IN THIS SECTION

1. **Guidelines Code A: Confessional Statements**  
   Page 65

2. **Guidelines Code B: Prosecution Witness Statements**  
   Page 71

3. **Guidelines Code C: Financial Record**  
   Page 79

   Page 99

5. **Guidelines Code E: Additional Evidence Concerning Relationship with Proscribed Organizations**  
   Page 113
GUIDELINES CODE: A
CONFESSIONAL STATEMENTS
## CODE A: CONFESSIONAL STATEMENTS

**IN THIS SECTION**

1. Evidentiary Value and Relevancy of Confessional Statements 67

2. General Guidelines 68
   a. Guidelines for the Investigating Officer 68
   b. Guidelines for the Prosecutor 69
   c. Guidelines for the Magistrate/Trial Court 69
If recorded in accordance with law, a confession becomes admissible in evidence and a conviction may be based on the same. Confessions before the Police not Admissible as Evidence
- Art.38 and 39 of Qanoon-e-Shahadat Order, 1984 state that confessions to a police officer or to anyone else while in custody of a police officer are not admissible as evidence.
- As a result, a confession made to a police officer during investigation of a money laundering offence under AMLA will not also be admissible as evidence.

Conditional Admissibility under Sec 21-H of Anti-Terrorism Act 1997
- As aforementioned, under the normal trial process, confessions made in front of the police are not admissible. However, these confessions have conditional admissibility under the Anti-Terrorism Act 1997 (“ATA”) if the evidence produced raises the presumption that there is a reasonable probability that the accused has committed the offence.
- This conditional admissibility of confessions made before police under the ATA will only apply to offences under the ATA itself, including Section 11-F (5), 11-H to 11-K of the ATA.
- A recent Supreme Court judgment, Nadeem Hussain and others v. the State held that the statements given by suspects to the police are excluded under section 21-H of the Anti-Terrorism Act, 1997 in all cases of terrorism. The law limits the admissibility of such a confession before the police, stating that there must be additional evidence, including circumstantial evidence, which must adequately connect the accused individual with the claimed offence. Conditional admissibility of a confession before the police is contingent upon the availability of some other evidence linking the accused person with the alleged offence, but in the present case, all other pieces of evidence relied upon by the prosecution against the appellant had utterly failed to do so.
- In Muhammad Latif v. The State, the Court held that since there was no hindrance in the chain of custody of circumstantial evidence and since the extra-judicial confession was credible, the extra-judicial confession corroborated the circumstantial evidence and consequently the plea by the accused was dismissed and the death penalty was upheld by the Supreme Court.

A Confession may be Considered Circumstantial Evidence against Co-Accused
- In Mobashar Ahmad v. The State, the Supreme Court held that in a joint trial, if a confession of one accused was proved under Article 43 of the QSO, the same might be taken into consideration as circumstantial evidence against the co-accused. The conditions necessary for the application of Article 43 of QSO are:
  - The accused and co-accused must be jointly tried for the same offence.
  - The joint trial must be permissible by law.
  - Both accused and co-accused must be affected by the confession.
- However, before relying on the statement or confession of a co-accused, the court should corroborate it with other evidence available on record.

Conviction may Rest Solely on a Judicial Confession
- Section 164 of the Code of Criminal Procedure, 1898 (“CrPC.”) empowers the Magistrate to record any statement or confession made to him in the course of an investigation.
- In Tanveer Ahmed v. The State, the High Court held that if a judicial confession is honest and is voluntary it can be made the sole basis for a conviction. Furthermore, such a confession does not lose its evidentiary value even if the same is retracted independent corroboration from a direct and indirect source of evidence.
In *Hashim Qasim v. The State*, the Supreme Court highlighted the prerequisites of acceptance of confession by the accused. It found that for accepting a confession, two essential requirements must be fulfilled; first, that the confession was made voluntarily and was based on true account of facts leading to the crime and, second, the same was proved at the trial.

In *Muhammad Ismail v. The State*, the Supreme Court found that a retracted judicial confession, unless corroborated, cannot be relied upon.

Section 265-J CrPC states, “The statement of a witness duly recorded under Section 164, if it was made in the presence of the accused and if he had notice of it and was given an opportunity of cross-examining the witness, may, in the discretion of the Court, if such witness is produced and examined, be treated as evidence.”

**General Guidelines**

**a. Guidelines for Investigating Officer**

- The Investigating Officer must write an application to the Magistrate for recording the confession of an accused.
- The confessional statement of the accused is recorded under Section 164 of the Cr.P.C. by a magistrate, and the procedure for it is given under Section 364 of the Cr.P.C.
- It is advisable that the confessional statement of an accused be preferably recorded by the concerned Magistrate and not by the Investigating Officer under Section 161 CrPC.
- Before producing an accused in the Court, the Investigating Officer shall verify each and every fact disclosed by the accused under Section 161 CrPC. (Till then, his confession shall be considered as statement made under this provision).
- If any disclosure has been made by an accused under Article 40 of QSO, which leads to any evidence relevant to the case, the Investigating Officer shall preserve such evidence before sending the accused to the Magistrate.
- The state of mind of an accused at the time of recording the confession must be included in the case diary of the police station.
- The Investigating Officer must record the confession in the daily diary of the police station when recording a confession under Section 161 CrPC.
- The accused should not be handcuffed while he is making a confession before an Investigating Officer.
- The Investigating Officer while recording a confessional statement must observe all legal formalities that a Magistrate has to observe under Section 164 CrPC. He must give the person giving the confessional statement time to reconsider his statement.
- Any person who is not a Senior Police Officer, must be asked to leave the premises where the accused records his confession.
- As per the Lahore High Court Rules and Orders Volume 3, the Investigating Officer must satisfy himself that the person making the confession has notice of the fact that he is making a confession.
- The Investigating Officer recording the confession must also satisfy himself that the confession has been made voluntarily.
- Every confession must be signed by its maker after he is satisfied that the Investigating Officer has written the correct version of his account.
- Confessional statements must not be exculpatory.
- For conditional admissibility of confession to the police under Section 21H of the ATA, the following is advised:
  - Confession must be made by the accused during investigation without being compelled, and before a police officer not below the rank of a District Superintendent of Police (DSP)
  - For the conditional admissibility of confessions, the DSP, before recording the confession, must explain to the person confessing that he is not bound to make a confession and that if he does so, it may be used as evidence against him.
  - The DSP must raise a reasonable presumption by gathering the opinion from all facts and circumstances of the case, the accused has made a true confession in respect of his guilt.

---

39 Ibid.
40 Hashim Khan v. the State 2017 SCMR 986
41 Muhammad Ismail v. the State 2017 SCMR 8198
• The DSP, when recording the confession, must make a memorandum at the foot of such record to the following effect:
   “I have explained to (...name...), that he is not bound to make a confession and that, if he does so, any confession he may make may be used as evidence against him and I believe that confession was voluntarily made. It was taken in my presence and was read over to the person making it and admitted by him to be correct, and it contains a full and true account of the statement made by him.” (Signed) Distt. Superintendent of Police.

• The police officer must not tender an oath to the accused making the confession.

• Special care for the preservation of confessional statement either in the central police record room or in the record room of the Sessions Court of the concerned district is advised. Confession if proved shall be conclusive proof of guilt.

• No police officer may offer a pardon. An accused person desirous of making a statement with a view to obtaining a pardon shall be told that no promise whatsoever can be made, but that if a statement is made and verified and found to be of sufficient importance to merit such action, the facts will be reported to the in-charge of prosecution of the district who shall take further steps in this regard. No steps may be taken in this connection by subordinate police officers without the previous sanction in writing of a gazetted police officer.42

• In case of an extra-judicial confession, the Police Officer must consider the following points:
   ▪ A delayed recording of statement of the person before whom the extra-judicial confession is made should be reasonably explained and;
   ▪ The relationship of the witness with the victim etc.
   ▪ The extra-judicial confession of each accused should be made separately and not jointly.

b. Guidelines for Prosecutor
• The prosecutor must scrutinize and analyze the confessional statement recorded by the Police Officer in accordance with the Lahore High Court Rules and Orders Volume III.

• Upon the recording of a voluntary confession, the prosecution should ensure judicial remand, as well as in the case where the accused refuses to confess before the magistrate. It should be ensured that the accused is not handed back over the police for remand, especially in the case where the accused refuses to confess before the magistrate.

• The prosecutor shall ensure the safe preservation of the confessional statement.

c. Guidelines for Trial Court/Magistrate
• The Magistrate should satisfy himself that the confession made by an accused is true and voluntary. In this regard, an endorsement certificate must also be issued.

• At the time of recording a confessional statement, the accused must not be handcuffed and no Police Officer whether related to the case or otherwise must be present in the Court.

• The Magistrate while recording the confession of an accused must consider the following, including a few features of Section 164, CrPC and otherwise:
   ▪ Statements or confessions made in the course of an investigation can be recorded only by a Magistrate of the first class or of the second class who has been specially empowered by the Provincial Government.
   ▪ Confessions must be recorded and signed in the manner provided under Section 364 CrPC.
   ▪ Before recording any confession, the Magistrate shall explain to the person making it that he is not bound to make a confession, and that if he does so it may be used as an evidence against him.
   ▪ No Magistrate shall record any confession unless upon questioning the person making it, he has reason to believe that it was made voluntarily. Failure to question has been held to vitiate the confession.
   ▪ The Magistrate should then allow the accused time for reflection, during which the police who brought him, the investigating officer and any other person shall not be allowed to have access to him. This time preferably should be at least one hour.43
   ▪ When the Magistrate records any confession, he shall make a memorandum at the foot of such record to the following effect: "I have explained to (name) that he is not bound to make a confession and that, if he does so, any confession he may make may be used as evidence against him and I believe that this confession was voluntarily

42 Police Rule 25.29, Police Rules 1934. Also mentioned in Police Prosecution Cooperation for Investigators and Prosecutors, Sindh Judicial Academy, Session 3: Confessional Statement.
43 Chapter V-C of The Federal Capital Criminal Court Circulars; Also mentioned in Police Prosecution Cooperation for Investigators and Prosecutors, Sindh Judicial Academy, Session 3: Confessional Statement.
made. It was taken in my presence and hearing and was read over to the person making it and admitted by him to be correct, and it contains a full and true account of the statement made by him” - (Signed) A.B. Magistrate.

- It is not necessary that the Magistrate receiving or recording a confession or statement should be a Magistrate having jurisdiction in the case.
- Any confessional statement of the co-accused may be recorded by a Magistrate in the presence of the other accused, and the other accused will be given an opportunity of cross-examining the co-accused making the confessional statement.

- The accused will be sent to a judicial lockup after the confessional statement is recorded.
- A certified copy shall be given to the prosecutor for his record and the Investigating Officer for the police file, and the original confessional statement should be preserved with great care and caution till the finalization of the case in the record room of the Sessions Judge.
- Special care should be taken when women and children are produced by the Police before the Court for recording their confessions as stated in the Lahore High Court Rules and Order Volume III.
- The Magistrate may ask the following questions from the accused before recording his confessional statement in accordance with the Lahore High Court Rules and Order Volume III:
  - Do you understand that your statement is being recorded by a Magistrate, and that if you make a confession, it may be used as evidence against you?
  - How long have you been in police custody?
  - Do you understand that after making a statement before me you will not be remanded to police custody, but will be sent to the judicial lock-up?
  - Understanding these facts, are you making a statement before me voluntarily?
  - What are your reasons for wishing to make a statement?

- The Magistrate is required to make enquiries as to the circumstances leading up to the confession, and police officers shall invariably furnish, so far as is in their power, information required of them in this respect.  44
- One important point upon which the Magistrate should invariably question the accused person is as to the length of time during which he (the accused person) has been in the custody of the police. It is not sufficient to note the date and hour recited in the police papers at which the accused person is said to have been formally arrested.  45
- The confession should ordinarily be recorded during Court hours and in open Court.
- Each confession shall be recorded separately after observing all supra-mentioned formalities.
- When more than one person confesses or turns approver in a case, their confessions shall, if possible, be recorded by different Magistrates and they shall not be allowed to meet one another till their evidence has been recorded in Court.  46
- While recording the confessional statement by the Magistrate or by any other Court having power to record it, the whole of such confession including every question put to him and every answer given by him, shall be recorded in full, in the language in which he is making the confessional statement, or, if that is not practicable, in the language of the Court or in English, as provided under Section 364, CrPC. In that case, it shall be explained to the confessor.
  - Such record shall be shown or read, to him, or if he does not understand the language in which it is written, shall be interpreted to him in a language which he understands, he shall be at liberty to explain or add to his

45 Chapter V-C of The Federal Capital Criminal Court Circulars; Also mentioned in Police Prosecution Cooperation for Investigators and Prosecutors, Sindh Judicial Academy, Session 3: Confessional Statement.
GUIDELINES CODE: B

PROSECUTION WITNESS STATEMENTS
CODE B: PROSECUTION WITNESS STATEMENTS

IN THIS SECTION

1. Evidentiary Value and Relevancy of Witness Statements 73

2. General Guidelines 73
   a. Guidelines for the Investigating Officer 73
   b. Guidelines for the Prosecutor 74
   c. Types of Prosecution Witnesses in Money Laundering Cases 75
Evidentiary Value and Relevancy

- Witness statements before courts, if recorded in accordance with the legal formalities and if it withstands cross-examination, may form the exclusive basis for a conviction.
- Witness statements may be recorded by police officers under Section 161 CrPC., or by the Magistrate under Section 164 CrPC.

Admissibility and Evidentiary Value of the Statements to the Police

- Witness statements recorded under Section 161 CrPC. before the police may not be used by the prosecution for any purpose at trial. However, they can be used by the accused, upon request to the Court, to contradict the witness if he/she testifies in the trial. The Qanun-e-Shahadat Order 1984 notes that previous statements of a witness may be used to contradict the witness (Art. 140) or to impeach his credit (Art. 151(3)).
- Statements of witnesses already recorded by a Police officer under Section 161 CrPC. can be supplemented at a later stage of the investigation if so required.
- A witness may wish to narrate further information which he learns about after recording his initial statement or may wish to offer information about events or facts which occurred after the recording of the initial statement under Sec. 161 CrPC.
- In *Nasir Ahmad v. State*, the relevance of witness statements was discussed. The accused, during his statement under Section 161 CrPC., had admitted that he was part of an unlawful assembly with a specific role. The Peshawar High Court ruled that the statement of the accused recorded under Section 161 CrPC. could have been taken into consideration, when the occurrence was an unseen one.

Admissibility and Evidentiary Value of the Statements to the Magistrate

- The value of such a statement recorded before a Magistrate is that it becomes admissible as evidence at trial. However, to ensure that the principle of audi alteram partem or that ‘no person is condemned unheard’ is adhered to, the Magistrate can only record such a statement in the presence of the accused. This allows the accused to cross-examine the witness and to contradict or provide an alternative explanation of the events stated by the witness.

General Guidelines

a. Guidelines for the Investigating Officer

- In recording statements under 161 CrPC., the Investigating Officer should take great care to ensure prompt recording of witness statements. A delay in the recording of a witness statement can be damaging to the prosecution of the case. It is important that witness statements are recorded without delay as soon as possible after the registration of the First Information Report (FIR) or at the time of recovery or evidence collection, as the case may be. In cases where delay does take place, this should be accompanied by a reasonable explanation duly noted in the case diary. Lacking a reasonable explanation for the delay, the court may view the witness and his/her statement with suspicion which may undermine the entire case.
- The Investigating Officer should ensure that the witness has all the relevant qualifications of competency as required by Article 3 of QSO and at the same time, ensure that the witness would deliver a qualitative account before the Court to be able to withstand cross-examination.
- Article 3, QSO: The law regarding who can be a witness in a criminal matter is broad. A Police officer “may examine orally any person supposed to be acquainted with the facts and circumstances of the case.” Article 3 of the QSO further notes that all persons are competent to be witnesses with some reasonable exceptions, including extreme old age, disease, etc.
- If the person whose attendance is required as a witness was ordered to join investigation in writing under Section 160 CrPC., the said order must be available on the police file.
- The Investigating Officer must ensure that statements recorded under Section 161 CrPC. are not signed or thumb-marked by the witness. As stated in Section 162, CrPC., statements made to the police officer, if reduced into writing, are not expected to be signed by the respective person.

---

47 See article 3, chapter IV, chapter X of Qanun-e-Shahadat Order 1984, and sectio 161, 164, chapter XXV of the Criminal Procedure Code 1898.
49 *Noor Muhammad v. The State*, 2020 SCMR 1049; *Muhammad Asif v. The State*, 2017 SCMR 486
Any such statement, or any record, or any part of the same cannot be used for any purpose at any inquiry or trial against the accused in respect of any offence under investigation as stated in Section 162, CrPC. It can only be used by the accused in order to confront the witness.

The Investigating Officer can use all modern devices for the purpose of investigation and recording of statement under Section 161 CrPC provided that the witness is visible to him.

Statements of witnesses must be recorded by the Investigating Officer promptly and verbatim as defined under Section 161 CrPC.

Any person who has been summoned as a witness under Section 160 would be bound to answer all questions relating to the case put to him by the police-officer other than questions the answers to which would have a tendency to expose him to a criminal charge or to a penalty or forfeiture as defined under Section 161 CrPC.

The Investigating Officer may reduce into writing any statement made to him in the course of the investigation and shall make a separate record of the statement of each person he records as defined under Section 161 CrPC.

The police officer must not offer any inducement, threat, or promise to any person making a statement, as stated in Section 163, CrPC.

The police officer must not prevent by any caution or otherwise, any person from making a statement during an investigation of his own free will, as stated in Section 163, CrPC.

The Investigating Officer is required to make a separate record of witness statements and include them in the case diary maintained under Section 172, CrPC.

Police Rules 1935, Rule 25.18 states that statements recorded by an Investigating Officer under Section 161 shall not form part of the case diary prescribed by Section 172, but shall be recorded separately and attached to the case diary.

Police Rules 1935, Rule 25.18 further states that the number of statements attached to a particular case diary, and the number of pages in each statement shall be noted in the case diary.

In a witness interview, leading questions, optional questions and multiple questions should be avoided so as not to suggest particular answers or create confusion.

Witness statements must be taken down promptly and verbatim. If these are missing, then it creates doubts as to the veracity of these statements, thereby harming the prosecution’s case. Police usually elaborate upon witness statements that later do not corroborate with circumstantial or documentary evidence, thereby weakening the prosecution case.

The Investigating Officer (IO) must be available before the Court during the entire proceedings of the trial of the case which he has investigated.

Investigating officers should also consider the possibility of recording a statement under Section 164 (which can become evidence during trial even if the witness does not want to give evidence anymore) for witnesses they fear may retract from their police statements during trial. Punjab Prosecution has used this tactic in rape cases as a majority of rape case victims/survivors and their families are pressured into resiling from their previous statements – there can be a similar kind of pressure, if not more, in terrorism cases as well.

b. Guidelines for Prosecutor

- The Prosecutor must look at the relevancy of evidence to the fact in issue, its admissibility and its credibility and quality.
- The criminal character and demeanour of the accused is also relevant, as well as any aspect of the accused’s character which casts doubt on the guilt of the accused. Similarly, his past criminal record is also relevant. The prosecutor must bring the attention of the court to such information.
- The prosecutor must prepare the IO and properly scrutinize and professionally present him before the Court.
- The prosecutor must know what examination-in-chief is, and what types of questions can be asked.
- Hostile Witnesses: If the witness becomes hostile or retracts his earlier statement, the prosecutor must apply to the court for initiation of proceedings. KP Guidelines and Punjab Guidelines specifically explain how to handle witnesses who retract from their previous statements. The relevant portions of those guidelines are excerpted below:

50 For more details on this and other witness interviewing techniques, see “Chapter 9: Witnesses and Witness Statements”, Handbook of Criminal Investigation in Pakistan (2021), National Police Bureau & Ministry of Interior, GoP.
51 Interview with ATC Judge, (Karachi, 25 July 2017).
Khyber Pakhtunkhwa Guidelines

“15(a). During examination (examination-in-chief, cross-examination and re-examination), in dealing with witnesses who have deviated from their previous statement given during investigation, a prosecutor must consider the following course of action:

i. If the witness has wholly deviated from the prosecution story by either denying giving a police statement during investigation or by showing unwillingness to support any aspect of the prosecution story, the prosecutors should consider declaring the witness hostile and impeaching his/her credit by invoking provisions of Article 151 of Qanon-e-Shahadat Order, 1984.

ii. If the witness has supported key aspects of the prosecution story but has suppressed some facts or made some candid admissions in favour of the accused, the prosecutor should consider invoking the provisions of Article 150 of Qanon-e-Shahadat Order, 1984, and asking the witness leading questions as to those facts without declaring the witness hostile.

iii. In all other situations, the prosecution should follow the provisions of Qanon-e-Shahadat Order, 1984, and other relevant laws/guidelines.”

Punjab Guidelines

The Office of the Prosecutor General Punjab issued a notification in 2018 regarding the implementation of Article 150 of the Qanun-e-Shahadat Order 1984 and witnesses who retract their previous statements. The text of the notification is as follows:

“The prosecutors during examination of prosecution witnesses in order to dilute the effect of candid statement occasionally made in favour of accused instead of relying upon Article 150 of the Qanoon-e-Shahadat Order 1984 (Question to own witness without declaring him hostile) get the witness declared hostile and subject them to cross examination under Article 151 of Qanoon-e-Shahadat Order 1984. Due to which prosecution puts the veracity of deposition in jeopardy.

I am directed to inform you to direct the prosecutors to invoke the provision of Article 150 of Qanoon-e-Shahadat Order 1984, in situation where witness does not negate prosecution story wholly and put questions through cross-examination without declaring him hostile. In all other situations appropriate decision may be taken in accordance with the provision of Qanun-e-Shahadat Order 1894.”

c. Types of Prosecution Witnesses in ML Cases

i. Approvers

In a money laundering scheme, especially ones launched by politically well-connected criminals seeking to launder large quantities of illicit funds, it is inevitable that a large number of accomplices, conspirators, and collaborators will be involved. Such a scheme cannot be adequately investigated unless the concerned LEA, IO, and prosecutor win over some of the accomplices to its side. Depending on the circumstances of the case, an accomplice can provide a valuable insider’s view of the money laundering scheme. In certain cases, failing to win over an accomplice may make it virtually impossible to gather evidence to gain a conviction.

Definition:

The formal definition of an accomplice is a person who participates in criminal activity but agrees to cooperate with the prosecution and testify against other defendants. In Pakistan, accomplices who are won over are referred to as “Approvers”.

In money laundering cases, approvers are usually individuals against whom a charge of abetment to the predicate offence and/or money laundering is made out. For example, they could be individuals who knowingly allowed the main defendants to register assets under their names as *benamis*, employees or associates who managed the front-business through which illicit funds were laundered, or professionals such as accountants, bankers, lawyers, and tax advisors.

---

52 See Gulzar Mehmood Khan v. Abdul Wahed (2016 CLC 848 Lahore); Muhammad Boota v. the State (1984 SCMR 560 SC); Irfan Ahmad v. the State (2019 P.Cr.L.J 1475 Lahore); AIR 1960 Guj. 9; AIR 1930 Cal. 139.

53 Also see Punjab Prosecution Department notification dated 5th June 2018.
consultants who assisted in laundering the money. Additionally, an approver can even be a main defendant responsible for generating the proceeds of crime, but who agrees to provide evidence against the hired professionals responsible for carrying out the money laundering. Approvers mostly agree to give evidence for the prosecution in return for leniency in sentencing, immunity from prosecution, or some other benefit. Usually, such approvers are used as informants in long-term investigations. They are expected to appear as prosecution witnesses, give statements, and participate in any other legal proceedings.

Selecting an Approver:
The prosecution must observe certain rules when targeting an accomplice to be won over:

<table>
<thead>
<tr>
<th>LEVERAGE</th>
<th>LESSER CULPABILITY THAN MAIN DEFENDANTS</th>
<th>ROLE OF APPROVER ESTABLISHED</th>
</tr>
</thead>
<tbody>
<tr>
<td>An IO or prosecutor must only target those accomplices to become approvers against whom there is sufficient leverage to induce cooperation. The prosecution must have already gathered evidence to convince the potential approver that he will face certain conviction and that his sentence can only be mitigated through full cooperation.</td>
<td>The level of the approver’s involvement in the money laundering operation should be lesser than that of the main defendants. The prosecution should first try to obtain cooperation from those who are minimally culpable and then ascend through the hierarchy of the money laundering enterprise till the point that there is sufficient evidence to establish guilt of the main defendants beyond a reasonable doubt.</td>
<td>The prosecution must satisfy itself that the approver is prima facie connected with criminal activity, that he bore some relationship with the primary defendants, and that he played some role in furthering the money laundering operation.</td>
</tr>
</tbody>
</table>

Approvers’ Evidence Must be Corroborated
Pitfalls in the case because of overreliance on the evidence provided by an approver should be avoided at all costs. When relying on the evidence of an approver, a basic principle that must be observed: All evidence from an approver must be corroborated. This is despite the existence of the provision under Article 16 QSO which allows for an accused to be convicted based on an approver’s uncorroborated testimony.

Nevertheless, an approver’s credibility and the veracity of his evidence must be determined by corroborating it with the statements of other witnesses or through documentary evidence such as records of financial transactions, banking records, digital evidence, call records, emails, or messages.

ii. Independent Witnesses
Most money laundering or terrorist financing operations maintain a certain level of interaction with independent third parties, such as bankers, accountants, property dealers, businesspeople, lawyers, and government functionaries. These third parties may not necessarily be aware that the organization they are dealing with is a criminal enterprise. They may engage in legitimate business with the money laundering or terrorist financing outfit, especially if it was being run through a front-company or masquerading as a charitable organization. For example, the independent third party may have rented business premises to the outfit, exchanged currency on their behalf, or conducted property deals for them.

Useful material from independent witnesses can be obtained, such as information regarding the persons actively involved in running the criminal enterprise and its employees, its financial or business transactions, documentary records, and other material can be obtained.
iii. Informants

Most LEA’s have informants in the criminal underworld who regularly supply useful and credible information in return for compensation or favours. LEA’s maintain links with such informants for intelligence gathering only, not for gathering evidence to be used at trial. Since such informants are keenly interested in maintaining their anonymity, they will not give statements, appear as a witness, or participate in any legal proceedings. Moreover, they may hold back on any useful information that might reveal their identity as the source.
GUIDELINES CODE: C
FINANCIAL RECORD
CODE C: FINANCIAL RECORD

IN THIS SECTION

1. Evidentiary Value and Relevancy of Financial Records  81
2. How to Obtain Financial Evidence; Relevant Legal Provisions  81
3. General Guidelines  83
   a. Guidelines for Tracing Illegal Financial Transactions  83
   b. Guidelines for Transport of Evidence  85
   c. Detailed Table containing Summary of Financial Evidence Documents  85
1. Evidentiary Value and Relevancy

- Evidence can also be divided into categories of oral and documentary evidence. Article 2(c) of the QSO, 1984, states that evidence includes oral and documentary evidence. Oral evidence or testimonial evidence is, “a person’s testimony offered to prove the truth of the matter asserted.” Documentary evidence is, “evidence supplied by a writing or other document, which must be authenticated before the evidence is admissible.”

- Documentary evidence cannot be rebutted by oral evidence. A document once brought on record can be given effect to by the Court even in the absence of a plea by a party to such effect. The physical presence of a person may or may not be necessary. Merely production of documents may serve the purpose of investigation. Summons or orders include the place and time to produce documents.

- General Clause, Pakistan Penal Code

  - According to the General clause of the Pakistan Penal Code (PPC), a document is defined as “any substance by means of letters, figures or marks, or by more than one of those means, intended to be used, or which may be used, as evidence of that matter.”

  - This document could be a contract, a cheque, a power of attorney, or a map. It could also be a set of instructions or directions to a task or an event that can be used as an evidence in the court of law.

  - If a person is found with funds or other property which are disproportionate to his known source of income, this kind of evidence becomes directly relevant as circumstantial evidence. However, mere presence of unexplained funds or other property cannot be made basis of ML offence unless a nexus is shown with the predicate offence.

  - The use of evidence of an extravagant lifestyle can be very persuasive. However, it must be relevant and will usually be supportive of a case where the prosecution asserts that the accused has accumulated assets through criminal activity rather than through a legitimate activity. The evidence of such wealth, therefore, will have to be of probative significance to the issue in the case.

2. How to Obtain Financial Evidence; Relevant Legal Provisions

- All financial institutions, reporting entities, government functionaries, and authorities are required to render full assistance to an LEA for the purpose of an investigation for ML under S. 25, AMLA 2010.

- Checking of Assets Without Notification to the Owner: Prevention of Electronic Crimes Act (2016):

  - The Prevention of Electronic Crimes Act, 2016, (PECA) allows Courts to issue warrants to a law enforcement officers to seize and search through any data that ‘may reasonably be required’ for a criminal investigation. It also allows a law enforcement officer to require a person to hand over data without the production of a warrant if the officer believes that such data is ‘reasonably required’ for a criminal investigation. This power is entirely discretionary, with the only caveat being that the officer must provide notice to the Court of such a seizure within 24 hours of acquisition.

  - Section 32 of the Act provides for far-ranging powers to authorized officers to conduct searches and seizure of data. In so doing, they must follow guidelines as provided under Section 35. One such condition placed by the legislation is to take all precautions to maintain the integrity and secrecy of the information and data that has been seized or collected.

  - Section 39 allows for real-time monitoring and collection of data if a Court is satisfied that such monitoring and collection is necessary for a criminal investigation. This can go on for a period of 7 days. If the Court is satisfied as to the efficacy of the monitoring and is of the belief that continued monitoring is necessary, it may extend the surveillance period.

  - Section 42 allows the government to share any data obtained from its investigation with any foreign government or international agency if such sharing would, in the opinion of the Federal Government, further the aims of the Act.

- Obtaining Additional Records (21EE ATA/AMLA/IFTA)

  - Under the ATA, the Superintendent of the Police is authorized during an investigation to call for additional records to facilitate the inquiry process.
• The Police may either call for information from any person or require that person to produce or deliver any document or thing useful or relevant to the ongoing inquiry.
• After acquiring permission from the court, the CTD is also authorized to obtain information, records and bank statements from banks and financial institutions. This section is of particular use when investigating TF offences that have been committed via the formal banking channel.

• Mutual Legal Assistance ("MLA")
  - MLA under IFTA:
    - Section 31 of IFTA states that warrants obtained under the Act shall be executable in both Pakistan and foreign jurisdictions, either by direct approach to relevant service providers, or through a mutual legal assistance mechanism as is agreed upon between Pakistan and the relevant foreign state. Section 31(2) and 32 indicate that warrants (both those initiated domestically and those received from foreign states) shall be processed for execution by the designated agency or body\textsuperscript{63} as set out in the Act.
    - Prior to the promulgation of the Mutual Legal Assistance (Criminal Matters) Act, 2020 (MLA Act, 2020), there was no uniform process whereby requests—both those originating in Pakistan and those from abroad—could be processed, and instead such requests were handled on an ad-hoc basis through multilateral treaties such as the United Nations Convention against Transnational Organized Crime.
  - MLA under Section 19C of the ATA, 1997 and Section 9A of the AMLA, 2010
    - Section 19C of the ATA and Section 9A of the AMLA, which provide for the usage of special investigation techniques for the investigation of financing of terrorism, money laundering, and related predicate offences, do not contain provisions relating to execution of warrants outside of Pakistan. However, both sections provide for the creation of rules to regulate procedure and execution.
  - MLA under the Mutual Legal Assistance (Criminal Matters) Act, 2020
    - The MLA Act, 2020, was promulgated to regulate the procedure for the rendering and solicitation of mutual legal assistance in criminal matters. Assistance shall be provided on the basis either of the principle of reciprocity,\textsuperscript{64} or where such reciprocal agreement does not exist, on the basis of a notification issued in the official Gazette, with directions that the provision of the Act apply to a specific country.\textsuperscript{65}

• Powers under Special Legislation: Law Enforcement Agencies have powers under their special legislation. These powers are listed as follows:
  - FIA: The investigating officer has the power to obtain and access records held by FIs, DNFBPs and other commercial entities under Section 5 of the FIA Act 1974.
  - ANF: Section 21 of the CNSA allows the ANF to search persons and premises, to call for information under Section 6 of ANFA, and to secure information from any departments/institutions under Section 31 of the CNSA. Section 6(3) of the ANFA also empowers ANF officers (not below the rank of Inspector) to arrest, without warrant, any person who has committed, or against whom a reasonable suspicion exists that he has committed, any of the offences relating to Narcotics.
  - NAB: Sections 19 and 27 of the NAO 1999 empower investigators to call for information and search people and premises.
  - FBR-Customs: Sections 26, 165, 166 and 168 of the Customs Act, 1969, apply to FBR-Customs obligations to produce documents, provide information and give them power to examine persons, summon persons to give evidence and produce documents or things, and seize things liable to confiscation.
  - FBR-IR: Sections 175 and 176 of the ITO 2001 and Section 38 of the Sales Tax Act (1990) empower authorities of the Directorate General, Intelligence & Investigation, Inland Revenue to access computer systems of persons involved in ML and tax evasion. The relevant provisions under ITO 2001 are Sections 176 & 177 and 37 & 38(A) and (B) of the Sales Tax Act 1990 that enable the FBR-IR to obtain records held by any person.
  - Section 216(2) of ITO 2001 contains a non-obstante clause to bar authorities from being entitled to require production of any documents relating to this Ordinance. However, subsections (3), (4), (5), and (6) create several exceptions.

\textsuperscript{63} Section 3 of the Investigation for Fair Trial Act: ‘Designated Agency or Body’ means any one or more Agency or Body designated by the Federal Government through notification for the purposes of this Act, having capability for implementing warrant of interception.
\textsuperscript{64} Mutual Legal Assistance (Criminal Matters) Act, 2020, Section 3(2).
\textsuperscript{65} Ibid., at section 3(3).
Section 216(3)(n) of ITO 2001 creates an important exception which allows documents to be disclosed for prosecutions under the Pakistan Penal Code. While this provision was never specifically extended to cover Anti-Terrorism Act offences, Sections 109 or 34 of the PPC may be added to the ATA charge to invoke this exception.

FBR: Section 216(6) of ITO 2001 is an exception in the Ordinance that allows the FBR to provide documents to NAB.

- **General Law vs. Special Law: Override Effect**
  - Two special laws i.e. the ATA, 1997 and the ITO, 2001 contain an overriding clause (non-obstante clause) which gives them precedence over any other law for the time being in force. Generally, if there are two conflicting statutes, the courts try to save the operation of a statute by adopting the most harmonious interpretation of the statute.
  - If that is not possible, the courts generally agree that the statute which is later in time prevails as it is the last explicit will of the legislature. The corollary of this is that the earlier statute which is inconsistent with the last will of the legislature is impliedly repealed. This doctrine of implied repeal is, however, a last resort.
  - The Supreme Court has further found that where two or more laws operate in the same field and each contains an override clause, cases of such conflict have to be decided in reference to the object and purpose of the laws under consideration.
  - Hence, the bar enumerated in S.216 ITO, 2001 does not appear absolute. It already permits disclosure in cases under the Pakistan Penal Code, National Accountability Ordinance and disclosures by public servants.
  - AMLA, 2010 is a statute later in time and enjoys a dominant position as the last expression of the legislature’s will.
  - However, **AMLA is not subject to the provisions of ITO, 2001**, and has an overriding effect over it.
  - As the last expression of the legislature’s will, AMLA 2001 also reasserts the overriding status of the ATA 1997.

**General Guidelines**

**a. Guidelines for Tracing Illegal Financial Transactions**

**Methods of Tracing Financial Transactions**

- Direct: analysis of specific financial transactions.
- Indirect: employs circumstantial evidence.

**Financial Institutions**

Information from financial institutions can be used to:

- Identify witnesses and other evidence.
- Uncover criminal profits.
- Identify Criminal assets.
- Locate assets that can be used to satisfy judgement.
- Identify localities where assets are stored.
- Determine the lifestyle of an account holder.
- Determine the financial health of an organization.
- Determine the source of funds placed into the account.
- Determine the use of funds from the account.

**Tracing Financial transactions: Banks**

**Personal accounts**

- Usually have person’s name, address, telephone number, identification number, amount of opening deposit, and security data.

**Business accounts**

- Corporation and partnership accounts typically have resolutions/agreements attached that authorize drawers; might have articles of incorporation.

---

Negotiated (cancelled) cheques
- Contain amounts, payees, endorses
- Deposited cheque might show account number and bank deposited; names of institutions cheque travelled through
- Can be used to identify other accounts held by subject

Loan records
- We transfer records (amount, date, name)
- Electronic payment records (assets and locations, loans, properties owned)
- Loan records
- Credit or loan file
- The loan application, financial statements (BS, P&L) etc.
- Red flags include unusual loan repayments (odd amounts, accelerated payments, large paydowns)
- Tracing loan proceeds and payments can identify hidden assets or witnesses

Credit card records
- Show movement and habits
- Document travel and who subject carries out business with
- Charges might provide leads to identifying hidden assets (charges related to boats, planes, etc.)

Indirect Approach to Tracing
Net-worth method
- Used to prove illicit income circumstantially by showing that a person’s assets/expenditures for a given period exceed what can be accounted for from known sources
- Net worth - the difference between assets and liabilities at a particular point in time
- By comparing the subject’s net worth at the beginning and end of a period, you can determine the increase or decrease in net worth.
- Useful when assets or liabilities have changed-no financial records.

Methods for Performing a Net-Worth Analysis
Asset Method
- Use when the subject invests illegal funds to accumulate wealth/assets

Expenditures Method
- Use when the subject spends illicit income on consumables that would not necessarily cause an increase in net worth
- Use when subject has invested illegal funds to accumulate wealth and acquire assets/pay down debts.
- Causes net worth to increase year to year.
- Used when subject spends illicit income on consumables, therefore not increasing net worth
- Establish known expenditure for relevant year
- Identify all sources of funds available to subject including loans, gifts, and cash on hand
- Compare known expenditures and known sources of funds during given period
- If spending exceeded known income sources, unaccounted for funds may be inferred to come from illicit/hidden income.

Locating Hidden assets
Characteristics money launderers want:
- Liquid
- Untraceable
- Secure
- Accessible
Common assets hiding techniques
- Hiding in someone’s else name
- Pay down debt
- Transfer to tax havens
- Transfer to trusts
- Insurance products

Locating assets Stored Abroad
- Letters Rogatory: Formal requests by one country’s court to another country’s court.
- Mutual Legal Assistance: Processes by which countries request and provide assistance in law enforcement matters and enforcing foreign orders and judgements.

b. Guidelines for Transport of Evidence

Transport of Evidence
- The transportation to the laboratory or to an intermediate storage location prior to examination of the evidence is a crucial step. It is essential for the following conditions to be met to ensure the sanctity and admissibility of the evidence:
  - The evidence recovered needs to be stored in a cool and dry place.
  - The evidence needs to be placed in a secure area with controlled access.
  - The cost, distance, and timeframe need to be calculated when dispatching evidence.
  - The transportation and storage services used ought to be documented. A written receipt is usually issued for all evidence submitted to the laboratory.
  - A Road Certificate is to be issued for the transport of all items of evidence.
  - All activities have to be logged in the daily diary register to keep up the compliance standards that show fairness and integrity of an investigation.

Designated Agencies for Examination
- Designated agencies are expert agencies that the Government has appointed for consultation for particular matters.
- Each agency has its own set of experts for the following types of evidence;
  - Serologist, Pathologist, Toxicologist and Medical Officer
  - Chemical Examiner
  - Bomb Disposal Unit Expert
  - Ballistics Expert
  - Trace Evidence Examiner
  - Latent Fingerprint Examiner
  - Digital Evidence Expert
  - Document Examiner

[This “Guidelines for Transport of Evidence” section is also relevant for Guidelines Code D and Guidelines Code E].

c. Summary of Financial Evidence

The following table is a summary of different kinds of financial evidence that can be obtained for investigations of ML and TF offences in Pakistan.

A detailed explanation of all these sources along with template requests and sample documents of each specific piece of evidence can be found in “AML/CFT Toolkit Vol. II: Guidelines on Obtaining and Analyzing Financial Evidence in Money Laundering and Terrorism Financing Cases in Pakistan.”
<table>
<thead>
<tr>
<th>RELEVANT INSTITUTION/DEPARTMENT</th>
<th>EVIDENCE TYPE</th>
<th>EVIDENCE</th>
<th>INFORMATION AVAILABLE IN EVIDENCE</th>
<th>METHOD OF OBTAINING EVIDENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Securities and Exchange Commission of Pakistan</td>
<td>Documentary Evidence</td>
<td>License to NPOs/NGOs/INGOs</td>
<td>License to NPOs, NGOs, INGOs: Primary purpose of the organization. The source of its funding (not always mentioned). Date of grant/renewal of license. Duration of validity of license. The NFP Form 1 contains complete details of the management including: Brief objects of the association. If the association already existed at the time of registration: old name of the association and its objects, registration type (society, trust, etc.), registration authority, and statement of charitable work already undertaken. Complete details of the management and relevant stakeholders including: - Members - Directors - Chief Executive Officer - Auditors - Bankers - Authorized Representatives - Financers - Other Intended Fund Providers. Details of their Current and Permanent Addresses. Copies of valid CNICs/NICOPs (copies of passports of foreign nationals). NTNs of Directors.</td>
<td>Evidence can be obtained from Registrar/Additional Registrar concerned at the Company Registration Office (CRO) through the Commissioner concerned at SECP (HQ). In addition, most of the information can be obtained from e-portal of the companies/NPOs/ NBFCs/NBMFCs which are registered with the SECP.</td>
</tr>
<tr>
<td>RELEVANT INSTITUTION/DEPARTMENT</td>
<td>EVIDENCE TYPE</td>
<td>EVIDENCE</td>
<td>INFORMATION AVAILABLE IN EVIDENCE</td>
<td>METHOD OF OBTAINING EVIDENCE</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------</td>
<td>----------</td>
<td>----------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Details of donations by members and directors</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Curriculum Vitae of members, directors and CEO</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Names of other associations/companies where the directors/members/CEO hold any position</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Forecasts of annual income and expenditure, including expected sources of income</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Application to Obtain permission submitted by prospective NBFC/NBMFC</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Full details, including professional qualifications, NTN, present occupations and evidence of payment of income tax, of all sponsors, directors, CEO, chairman of Board etc.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Names, addresses and annual accounts of all other organizations where the sponsors, directors, CEO and chairman have previously served.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Amount of capital (money or otherwise) contributed by each sponsor</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Feasibility report (financial forecasts for the company)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Latest CIB report in respect of sponsors</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Application for grant of license submitted by prospective NBFC/NBMFC</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Date of incorporation as a limited company</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Names and addresses of directors and number of shares held by each of them</td>
<td></td>
</tr>
</tbody>
</table>
- Directors’ interest, direct or indirect, in any other company with details of such interest
- Details of persons or group controlling the company including major shareholders with number and value of shares held
- Details of qualified staff engaged
- Reasons for selecting the proposed place of business with statistical data

- License for NBFC/NBMFC
- While most of the relevant information would already have been covered through applications to obtain license, the license itself confirms the following information:
  - Permitted activities of the company
  - Permission from relevant authorities to use funds in specified areas.
  - Duration of license and whether it is renewable or not.

- Certificate of Incorporation contains:
  - Corporate Unique Identification Number
  - Name of Company
  - Whether limited by guarantee or by shares
  - Date and city of incorporation

- Memorandum of Association contains
  - Name of the organization
  - Registered office address
  - Primary purpose of the company
  - Activities that the company cannot undertake
<table>
<thead>
<tr>
<th>RELEVANT INSTITUTION/DEPARTMENT</th>
<th>EVIDENCE TYPE</th>
<th>EVIDENCE</th>
<th>INFORMATION AVAILABLE IN EVIDENCE</th>
<th>METHOD OF OBTAINING EVIDENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Names and particulars of members</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Permission to obtain funds</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Effect of dissolution of company</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Articles of Association contain:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Types of sources of funds of the organization</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Procedure for transfer of shares (in case of company with share capital)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Powers of Board of Directors</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Rules for appointment/removal of the Chief Executive Officer</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Rules for appointment of auditors</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Rules for appointment/removal/suspension of bankers</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Rules for appointment of authorized representatives</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Procedures to maintain minute books for meetings</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Rules relevant to books of accounts, annual accounts and their inspection by members</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Other business Rules</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Application for Incorporation: FORM II contains</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Company information, including correspondence address and registered office address</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Complete details of subscribers, directors and CEO, including their nationalities, addresses, present occupations etc. Copies of their CNICs/passports are also attached.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• If a subscriber to shares is a foreign company,</td>
<td></td>
</tr>
</tbody>
</table>
the profile of company, detail of its directors, their nationality and country of origin, and certified copies of company’s charter, statute, memorandum and articles of association are also attached.

- Form A and Form B contains complete details of the organization, including:
  - Registered office address of company and its principal line of business
  - Number of shares that have been paid for by members, and any sale/purchase of shares that took place during the year
  - Complete details (including name, address, nationality, shares, NIC) of:
    - Members
    - Directors
    - Chief Executive Officer
    - Chief Financial Officer
    - Company Secretary
    - Legal Advisor
    - Auditors
    - Authorized Representatives
    - Copies of valid CNIC/Passports

- Form 2 contains details of company/members of the board of directors/promoters
- Forms 31 and 32 contain information on substantial offshore investments
- Forms 43 and 45 contain details on ultimate beneficial owners.
<table>
<thead>
<tr>
<th>RELEVANT INSTITUTION/DEPARTMENT</th>
<th>EVIDENCE TYPE</th>
<th>EVIDENCE</th>
<th>INFORMATION AVAILABLE IN EVIDENCE</th>
<th>METHOD OF OBTAINING EVIDENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal Board of Revenue (FBR)</td>
<td>Digital/Documentary Evidence</td>
<td>Form 181 • Income Tax Return Form • Statement of assets and liabilities (Wealth Statement)</td>
<td>Form 181 contains complete particulars of taxpayer, including CNIC details, passport details, addresses whether permanent or temporary, mobile number(s), bank accounts and their numbers, authorized representatives (e.g. income tax practitioners) for the purposes of filing of returns and statements etc.</td>
<td>Information can be applied for and obtained from Chairman Federal Board of Revenue. (An application should be written to the FBR in the template given below. A clear reference should be made to Section 216(3)(n); Section 21EE; or Section 25 of AMLA depending on the circumstances.), Director Excise (Islamabad), DG Excise and Customs (Provinces), Concerned Collectorate or Directorate (I&amp;I) in case of unregistered or benami vehicles, Concerned Collector (Customs) Model Custom Collectorate FBR</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Order under section 120 of Income Tax Ordinance, 2001 • Order to grant/refuse registration • Foreign income &amp; assets statement for resident individuals • Sales Tax Returns under Sales Tax Act 1990 • Provincial and ICT Sales Tax on rendering of services • Goods and Services under Schedule of the Federal Excise Act 2005</td>
<td>From income tax returns, we can secure the following information and documents: • Names, contact details, address of person. • Incomes and its sources declared. • Foreign remittances • Donations and Zakat • Taxable incomes and non-taxable incomes. • Taxes paid • Date of submission of tax returns. • Authorized representative (as mentioned in Form 181) From the wealth statement, one can secure the following information and documents: • Person’s list of total assets and their cost value on June 30th of every year. • Person’s total liabilities along with details to whom payable, reason of liabilities and date of subsequent payments. Investigating Officers can explore link to person/s to whom amounts are payable.</td>
<td>FBR Maloomat: Most of the information can be obtained from e-portal with effect from July 1, 2014 and onward.</td>
</tr>
</tbody>
</table>
• Complete details of assets of Person’s spouse, minor children and dependents along with source of assets acquired.
• Complete details of liabilities of Person’s spouse, minor children and dependents along with details to whom payable and reason of liabilities.
• Reconciliation of assets and liabilities which shows sources of funding / incomes, payments made along with sources of payments made.
• Agricultural income for the purposes of reconciliation of wealth (whether challan for provincial tax has been paid etc.)
• Donations (through banking channels or otherwise etc.)

• Foreign income & assets statement for resident individuals contains:
  • List of offshore assets like moveable / immovable properties.
  • Off-shore bank accounts details.
  • List of shares or interests held in foreign companies.
  • List of foreign sources of income/s.
  • Foreign assets transferred by the person to any other person during the tax year

<table>
<thead>
<tr>
<th>RELEVANT INSTITUTION/DEPARTMENT</th>
<th>EVIDENCE TYPE</th>
<th>EVIDENCE</th>
<th>INFORMATION AVAILABLE IN EVIDENCE</th>
<th>METHOD OF OBTAINING EVIDENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Excise Departments] Vehicle Registration</td>
<td>• [Excise Departments] Vehicle Registration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• [Excise Departments] Urban property tax (PT1, PT2)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FBR Maloomat Portal</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Import Export Records</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[Excise Departments] Vehicle Registration: The authorities concerned (Investigating
<table>
<thead>
<tr>
<th>RELEVANT INSTITUTION/DEPARTMENT</th>
<th>EVIDENCE TYPE</th>
<th>EVIDENCE</th>
<th>INFORMATION AVAILABLE IN EVIDENCE</th>
<th>METHOD OF OBTAINING EVIDENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Officers) can access details including particulars of the owner of vehicle, date of purchase and date of registration of vehicle etc.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• [Excise Departments] Urban property tax (PT1, PT2): authorities’ concerned (Investigating Officers) can access person’s details which includes all details and particulars of the person, value, area, type of property (commercial or residential).</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• This contains all details from the year 2017 and onward like, assets purchased/sold, cars purchased/sold, banking transactions, taxes paid or deducted by others, shopping and travel details etc. FBR is in process to update the same from July 1, 2014</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Import Export Records: The authorities’ concerned (Investigating Officers) can access WeBOC details of the company. Federal Board of Revenue (FBR) has introduced its Web Based One Customs (WEBOC) System for filing Goods Declarations (GDs) etc. and online clearance of imports and exports.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Therefore, information provided by the company/individual for WeBOC registration, and subsequently provided for obtaining clearance of imports and exports can be accessed by Investigating Officers to determine any linkages with off-shore companies or suspicious entities.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RELEVANT INSTITUTION/DEPARTMENT</td>
<td>EVIDENCE TYPE</td>
<td>EVIDENCE</td>
<td>INFORMATION AVAILABLE IN EVIDENCE</td>
<td>METHOD OF OBTAINING EVIDENCE</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------</td>
<td>----------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Financial Institutions / Banks etc. | Documentary Evidence | • Deposit Slips  
• Bank Locker Application and Record  
• Account Opening Documents  
• Bank Account Statements  
• Wire Transfers  
• (IR Documents)  
• Mobile Wallet Accounts  
• Letters of Credit  
• Credit Facilities and Financing | • Deposit Slips are used to acknowledge deposit of both cash and instruments (including inter and intra-bank cheques, bank drafts and other paper instruments) in an account holders’ account by the bank. Deposit Slips show:  
• For payee: Date, Name and bank accounts details of the payee.  
• For the depositor: Date, Name, CNIC number, contact number, signature, city and bank branch from where the cash is deposited or funds are being transferred (as stamp), purpose of deposit / funds transfer (not necessarily available in all banks), date of deposit / funds transfer and biometric record or copy CNIC of the depositor or the account number of the depositor.  
• In case of online bank transfers: Name of transferor, CNIC number, contact number, bank accounts details, purpose of funds transfer (where available) and date of funds transfer. | For banking documents, the Investigating Officer needs to Approach the head office of the relevant bank. |

- **Bank Locker Record:**  
  - Name, CNIC number and contact number of customer  
  - Bank accounts details of customer  
  - Branch wherein locker is being operated  
  - Authorized persons who can access the locker
<table>
<thead>
<tr>
<th>RELEVANT INSTITUTION/DEPARTMENT</th>
<th>EVIDENCE TYPE</th>
<th>EVIDENCE</th>
<th>INFORMATION AVAILABLE IN EVIDENCE</th>
<th>METHOD OF OBTAINING EVIDENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Credit card information:
  - Account opening form, / credit card application form
  - Specimen signature card
  - CNIC/NICOP/POC/proof of identity and proof of income (for primary card holder)
  - Monthly Credit Card Statements to see purchases made using the card

- Bank Account Statements:
  - Account Number,
  - Title of account,
  - Bank and branch name
  - Mailing address of account holder (where hold mail instructions are not given),
  - Record of transactions (date deposits/withdrawals and balance after each transaction).

- Wire Transfers (IR Documents): SBP Regulation - 11 minimum information required to process a wire transfer has been provided for remitter, beneficiary & intermediary bank.

- eMobile Wallet Accounts/Branchless Banking Accounts: Investigating Officers can request for mobile banking records to determine trail of transactions – purchases through account or transfers to other accounts.
<table>
<thead>
<tr>
<th>RELEVANT INSTITUTION/DEPARTMENT</th>
<th>EVIDENCE TYPE</th>
<th>EVIDENCE</th>
<th>INFORMATION AVAILABLE IN EVIDENCE</th>
<th>METHOD OF OBTAINING EVIDENCE</th>
</tr>
</thead>
</table>
| State Bank of Pakistan          | Documentary Evidence | • Credit Information Bureau Report | • Letters of Credit: Information of importer and exporter, third parties, beneficiaries, invoice containing details of goods and services, price, shipping documents, packing list etc.  
• Credit Facilities and Financing: Investigating Officers can request banks for all financing agreements executed between bank and customer. The agreement will consist of details of the type and amount of finance, repayment method and period, security/collateral held, markup, and other information. Investigating Officers should specifically note details of securities/collaterals held which may reveal hidden properties of the customer. There may be multiple agreements between the customer and the bank, and/or multiple agreements between multiple banks and a customer. | Relevant department in the State Bank of Pakistan. |
| Registrar Trust                 | Documentary Evidence | Trust Deed                  | • Complete details and particulars of trustees, beneficiaries, and ultimate beneficiaries  
• Purpose of trust  
• Date of registration of trust | The Registrar or Joint Registrar (concerned), Trust Registration Office |
<table>
<thead>
<tr>
<th>RELEVANT INSTITUTION/DEPARTMENT</th>
<th>EVIDENCE TYPE</th>
<th>EVIDENCE</th>
<th>INFORMATION AVAILABLE IN EVIDENCE</th>
<th>METHOD OF OBTAINING EVIDENCE</th>
</tr>
</thead>
</table>
| Registrar Societies and Partnership Firms | Documentary Evidence | Relevant Documents of Societies/Partnership Firms/LLPs | • Partnership Deed and application for registration of firm.  
• Names and particulars of partners, and date of joining the firm  
• Roles and responsibilities  
• Contribution and share of the partners, and future ratio of sharing profits  
• Effective date of partnership  
• Principal line of business of firm  
• Registered office of partnership  
• Name and details of managing partner  
• Memorandum of association, rules and regulations of society and registration certificate  
• Registered office of society  
• Purpose of the society  
• Types of sources of funds  
• Number of members of council of society, and their names and addresses  
• Date of registration | The Registrar, Societies/Partnership Firms, Deputy Commissioner’s Office, Islamabad. |
| Ministry of Interior and Economic Affairs Division | Documentary Evidence | Work Permit and Memorandum of Understanding (MoUs) of INGOs | • Details of INGO and its members  
• Annual Plan of Action  
• Sources of funding/budget  
• Funding guarantee letter/donor commitment  
• Registered office address  
• Declaration of assets  
• Scope of work  
• Bank account details | The Economic Affairs Division, Ministry of Economic Affairs, Islamabad.  
And Ministry of Interior, Islamabad |
<table>
<thead>
<tr>
<th>RELEVANT INSTITUTION/DEPARTMENT</th>
<th>EVIDENCE TYPE</th>
<th>EVIDENCE</th>
<th>INFORMATION AVAILABLE IN EVIDENCE</th>
<th>METHOD OF OBTAINING EVIDENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Tax returns and annual reports for last 3 years (if it is an existing NGO starting to receive foreign funds)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Tax credits available to the INGO</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Obligations of the organization</td>
<td></td>
</tr>
<tr>
<td>Land Record Regulatory Departments</td>
<td>Documentary Evidence</td>
<td>Land Record Regulatory Departments</td>
<td>The authorities’ concerned (Investigating Officers) can access complete details of asset holders (allottees, transferors, transferee) and their authorized representatives. Moreover, Investigating Officers can retrieve information of illegal housing schemes, approved architectural or development plans, encroachments and illegal sites or properties with missing files.</td>
<td>The letters need to be addressed to the Head of authorities mentioned in the description</td>
</tr>
</tbody>
</table>
| Accounting Firms | Documentary Evidence | Auditor’s Reports/Audited Accounts | • Auditor’s report will highlight any deficiencies or matters of concern  
• Audited accounts will include information of company’s assets and liabilities, and income and expenses.  
• Management Letter (ML) will include other control deficiencies found by the auditor, and management’s responses to those identified deficiencies. | Concerned auditors of the organization |
| Open Source Information | Digital Evidence | Open Source Information | • Adverse Media Checks: Also known as negative news checks, is the process of screening an entity (individual or corporate) | Online Research |
against news articles, legal prosecution or similar content that may affect the final risk by revealing their involvement in money laundering, terrorism, fraud, tax evasion, or other types of crimes. Financial Action Task Force (FATF) in its Risk-Based Approach Guidance identifies adverse media searches as a part of Enhanced Due Diligence (EDD) practice. Negative news can be derived for a variety of official news sources or unstructured data sources such as social media, internet forums, or databases.

- Bin list: The first 8 numbers on payment cards are known as the Issuer Identification Number (IIN) or Bank Identification Number (BIN), and they contain information about the card issuer and the card itself. Drop those numbers into a Bin Database site, and it will tell you a) what financial institution issued the card, b) the country the card was issued in, c) what network it belongs to (e.g. Visa or Mastercard), d) whether it is a credit or debit card, e) whether or not it is a prepaid card.
- SWIFT Code Lookup: A SWIFT code mentioned on a SWIFT message used in cross border transactions can be looked up online to determine a) bank b) branch c) city and d) country. First 4 characters are institutional code, next 2 are country code, next two are city
<table>
<thead>
<tr>
<th>RELEVANT INSTITUTION/DEPARTMENT</th>
<th>EVIDENCE TYPE</th>
<th>EVIDENCE</th>
<th>INFORMATION AVAILABLE IN EVIDENCE</th>
<th>METHOD OF OBTAINING EVIDENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>code and the next three (optional) are branch code or XXX if branch is not specified.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• World-Check: Refinitiv’s World-Check is a database of Politically Exposed Persons and heightened risk individuals and organizations, used around the world to help to identify and manage financial, regulatory and reputational risk. Investigating Officers can check search using names of individuals and organizations identified during investigation to determine whether they have been involved in money laundering or similar activities in any other part of the world. World-Check system can only be accessed through a paid subscription to its services.</td>
<td></td>
</tr>
</tbody>
</table>
GUIDELINES CODE: D
EXPERT ANALYSIS AND FINDINGS
CODE D: EXPERT ANALYSIS AND FINDINGS

IN THIS SECTION

1. D1: Interception and Surveillance [Definition; Evidentiary Value and Relevancy] 103

2. D2: Digital/Cyber Evidence [Evidentiary Value and Relevancy; General Guidelines] 105
   a. D2.1: Digital Equipment like Computer and Mobile Data 105
      i. D2.1.1: Call Detail Record (CDR) and Sim Data Registration 106
      ii. D1.1.2: Record from Social Media Companies 108
   b. D2.2: Audio Video Recording 108


4. D4: Forensics: Fingerprints and Handwriting 111
D1: INTERCEPTION AND SURVEILLANCE

1. Definition

**Interception** include-mails, SMS, IPDR (internet protocol detail record) or CDR and any form of computer based or cell phone-based communication and voice analysis. It also includes any means of communication using wired or wireless or IP (internet protocol) based media or gadgetry.  

**Surveillance**: data, information or material in any documented form, whether written, through audio visual device, CCTV, still photography, observation or any other mode of modern devices or techniques obtained under this Act; and (b) documents, papers, pamphlets, booklets.

- Any evidence obtained from modern devices or techniques is admissible as per Art. 164 of the QSO. Apart from the conventional oral or documentary evidence required to prove an offence, Pakistan’s criminal justice system has gradually acknowledged the admissibility of evidence that falls within the confines of this provision.
  - Furthermore, within the context of Section 19-C of the ATA, Section 27-B of the ATA allows convictions to be based on electronic evidence alone, provided that the Court is satisfied with its genuineness.
    - Such evidence must be forensically analyzed from the concerned forensic agency/wing [e.g. Punjab Forensic Science Agency]
- Under the QSO, such evidence may constitute documentary evidence within the meaning of Art. 2(1)(b) and (c) of the QSO.
- Alternatively, the same may be constituted as an electronic document/information under Art. 46-A of the QSO.
- Ultimately, however, the said evidence would have to be proven in accordance with the provisions of the QSO as a whole, and Chapter V of the QSO, in particular, which outlines provisions relating to documentary evidence.

2. Evidentiary Value and Relevancy

<table>
<thead>
<tr>
<th>PRINCIPAL LAW</th>
<th>OBJECTIVE</th>
<th>SECTION INCLUDED BUT NOT LIMITED TO</th>
<th>RELEVANT EVIDENTIARY PROVISIONS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Anti-Terrorism Act, 1997 | Data Collection and Analysis | Section 19C | • Art. 164 QSO  
• Section 27-B ATA  
• Art. 2(1)(b) and (c) QSO  
• Art. 46-A QSO  
• Chapter V QSO  
• Art. 59 QSO | ATA: The provision authorizes the Investigating Officer to use techniques including 'undercover operation, intercepting communications, accessing computer system and controlled delivery' for the investigation of financing of terrorism. Interception and surveillance under this provision may only be done for the investigation of financing of terrorism provided the IO has obtained permission from the Court. |

---

68 Symbolic/Non-Symbolic System Based Communications  
69 IFTA, 2013, Article 3(g)(ii); Symbolic/Non-Symbolic System Based Communications  
70 Ibid., Symbolic/Non-Symbolic System Based Communications  
71 Ibid., at Article 3(g)(ii).  
72 Guidance for what constitutes ‘investigation of financing of terrorism’ may be drawn from Section 2(z) read with 2(aa) of the ATA by analogy  
73 ATA, 1997, Section 2 (c).
| Anti-Money Laundering Act, 2010 | Section 9-A | • Art. 164 QSO  
• Art. 2(1)(b) and (c) QSO  
• Art. 46-A QSO  
• Chapter V QSO | Allows for the usage of modern investigative techniques in the investigation of financing of terrorism.  
**AMLA:** This provision also, to a great extent, mirrors Section 19C of the ATA. It stipulates that the investigating officer can apply to the Court\(^74\) for a warrant of interception and surveillance.  
Allows for the usage of modern investigative technique in the investigation of money laundering. |
| IFTA 2013 | Sections 1-39 | • Art. 164 QSO  
• Art. 2(1)(b) and (c) QSO  
• Art. 46-A QSO  
• Chapter V QSO | **IFTA:** The Directorate General Inter-Services Intelligence, the three Services Intelligence Agencies, the Intelligence Bureau and the Police are listed as Applicants under the Act,\(^75\) which empowers—and requires—them to approach the Federal Minister for Interior for permission to make an application to the Judge\(^76\) for the use of interception and surveillance. The application itself, in order to not jeopardize any ongoing investigation, will be presented to the Judge in-chambers\(^77\) by the authorized officer,\(^78\) wherein the judge shall consider whether the collection of evidence through such extraordinary means is necessary, and subsequently either issue or decline such warrant. The Act requires that the Judge essentially apply a threefold test in order to determine the issuance of a warrant:  
1. Would the warrant, if issued, enable the applicant to collect evidence?\(^79\) |

---

74 AMLA, 2010, Section 20.  
75 Investigation for Fair Trial Act, 2013, Section 3 (a).  
76 Ibid., at Section 3 (b): Judge means a Judge of the High Court  
77 Ibid., at Section 9 (1).  
78 Ibid., at Section 3(b): ‘Authorized officer’, means any officer, not below the rank of BPS-20 or equivalent who is working with the applicant and is notified under section 4 to represent the applicant when making application or taking up any proceeding under this Act;  
79 Ibid., at Section 10 (1) (a).
2. Is there a reasonable threat that a scheduled offence will be committed?\(^{80}\)

3. Would the warrant, if issued, cause undue interference with the right to privacy of persons and property?\(^{81}\)

Once this determination has been made, the Judge will issue a warrant for a duration of sixty days, which can then be re-issued for a further sixty days by the Judge after being shown sound reasoning for such an extension by the authorized officer.\(^{82}\)

If the Judge declines the issuance of a warrant, the applicant may approach the Chief Justice of the concerned High Court for constitution of a Division Bench of two judges for a hearing in-chambers to review said earlier decision.\(^{83}\)

---

**D2: DIGITAL/CYBER EVIDENCE**

**D2.1. Digital Equipment (Computer and Mobile Data)**

1. **Evidentiary Value and Relevancy**
   - See D1, except for provisions that apply specifically in the context of the IFTA, Section 19-C of the ATA and Section 9-A of the AMLA.
     - **CDs and USBs**: In *Sikandar Ali Lahsari vs. The State*, the Court noted that by virtue of the application of Section 27-B and Article 164 of the QSO, the accused was to be supplied the copies of CD and USBs in compliance with Section 265-C of the Code of Criminal Procedure, 1898.
     - **Digital Forensic Analysis**: Through respective Forensic Agencies.
       - In *Adnan Hafeez vs. The State*, the FIA seized three laptops, mobile phone and one PTCL Evo Wingle. These were then forwarded to the Forensic Science Agency for forensic analysis.

2. **General Guidelines**
   - For Guidelines on Transport of Evidence, see relevant sub-heading namely “Guidelines for Transport of Evidence” in Guidelines Code C.
   - Information on social media found through the Accused’s Computer and Mobile Phone:
     - *Asim Nawaz alias Kaleem Nawaz vs. The State*\(^{86}\)

---

\(^{80}\) Ibid., at Section 10(1)(b).

\(^{81}\) Ibid., at Section 10(1)(d).

\(^{82}\) Ibid., at Section 14.

\(^{83}\) Ibid., at Section 28.

\(^{84}\) Sikandar Ali Lahsari vs. The State, 2016 YLR 62.

\(^{85}\) Adnan Hafeez vs. The State, PLD 2016 Lahore 318.

\(^{86}\) Asim Nawaz alias Kaleem Nawaz vs. The State, 2019 PCLJ 920.
- The related evidence (audio files, graphic files and multimedia files) was inspected through the Punjab Forensic Science Laboratory
- Recovery Memo of the material from Facebook was made after printing the content.\(^{87}\)

Note: Prosecutor [where possible] must be consulted prior to presenting this evidence. Such evidence should only be raised if it is of a sufficient nature, can be proved, and is directly relevant to the case.

Email:
- In the recent judgment of *Taimoor Mirza v. Maliha Hussain*\(^{88}\) the Court made observations on digital evidence in the following manner:
  - “9. […] If it is established that any information communicated by a person from his account through email, Facebook, WhatsApp, twitter etc., the same may conveniently be referred during cross-examination. It is my considered view that even the courts can use electronic mail and WhatsApp for communication to a party in respect of service etc., as these are the medium from which the delivery of message and its perusal by the party can easily be established. Thus, any email written by a witness or addressed to him and received in his inbox is his document and the same can be used to confront him by just referring it or producing it if attention of witness is required to draw toward certain portion of the document. Even any other sorts of digital documents in the shape of messages, photographs or movie clips can be referred and used during cross-examination of a witness, provided it is established that the same had been shared by him on social media from his personal account.”\(^{89}\)

  - “10. […] In fact, email is a form of documentary evidence and the same can be admitted as evidence in court in the same way as other forms of documentary evidence. An email can be produced as a document in shape of hard-copy i.e., printout, but one may not consider an email or other form of electronic text message as a ‘smoking gun’ in favour of his case. This can be a particular issue and measures should be taken to protect the integrity and authenticity of email by digital signature (if available) and encryption etc… The major evidentiary issue for a trial judge arises in respect of a private digital communication to reach at a conclusion that the texts of electronic document were genuinely written by the other party or not. Besides getting some technical and expert assistance, a judge can overcome this problem of authentication of an e-mail or text message through different ways, which are:
    i. the adverse party admits that the texts were written by him.
    ii. a witness may come in witness box and say that he saw the message created.
    iii. characteristic of the message itself speaks that it was created by the author for whom it is claimed as author of the same.
    iv. circumstances of the case proof (sic) that it was created as claimed.
    v. a ‘reply authentication’ specially for e-mail, i.e. an electronic reply showing both parties e-mail addresses and text messages clearly indicating that the same was sent in response to the text message that was initially sent.

  - “11. Nevertheless, reliability of email or other electronically generated documents may be subject to attack but a party cannot be restrained to present it in the Court as a documentary evidence. The ultimate outcome of the above discussion is that the petitioner may confront the respondent with her previous statement either oral or in shape of document including digital document like email or any other form of electronically generated or created document communicated through the medium of internet.”

D2.1.1. CDR and SIM Registration Data

1. Evidentiary Value and Relevancy
- See D1, except for provisions that apply specifically in the context of the IFTA, Section 19-C of the ATA and Section 9-A of the AMLA.

---


\(^{88}\) Taimoor Mirza v. Maliha Hussain, 2020 CLC 1029.

\(^{89}\) Ibid.
Powers to require information:

- In terms of the power to call information, Section 21EE allows the Superintendent of Police, on the request of JIT can:
  - (e) require information or obtain record of telephone and mobile phone data, e-mail, MMS and CNIC and encrypted messages or any other information suspected to be linked in any manner with commission of an offence under this Act, from any service provider company of department.
- In addition, Section 25 of AMLA allows for the collection of information 'including but not limited to production of records, documents and information reasonably required by the investigating or prosecuting agency…'.
  - Together, the words including but not limited to and information reasonably required by investigating or prosecuting agency may be construed to mean that such information may be acquired by the authorities for assistance in their investigations.
  - Unlike the other two provisions, Section 25 of AMLA does not require a court order.
- Finally, in cases where the aforementioned powers may not be applicable, Section 94 of the CrPC. permits the LEAs to summon record or other things.

2. General Guidelines

- For Guidelines on Transport of Evidence, see relevant sub-heading namely “Guidelines for Transport of Evidence” in Guidelines Code C.

Process to be followed by the IO:

- Firstly, issue a letter to the concerned officer/authority for the issuing of CDR/Sim Registration Data/IMEI.
- Secondly, the IO is to prepare a recovery memo and insert the same into the case diary as per Section 172 of the CrPC.
  - At the time of receiving the relevant information, the IO would be required to have one witness accompanying them and have another witness from the concerned office attest to the production of said evidence as per Section 161 of the CrPC.; the same shall also be added to the zimni. The following cases shed light on the importance of adhering to this particular point: Witnesses in whose presence the information is conveyed or received are always important to prove a fact through its verification.
  - In Salman Alias Lamba and Another vs. The State, the Investigation Officer had collected CDR of the mobile phones recovered from the possession of the accused and completed process of verification of the SIMs and National Identity Cards issued by National Data and Registration Authority. Evidence of Police Officials was not trustworthy. No evidence had been produced to satisfy the Court that recovered cell phone SIMs were kept in safe custody. Records showed that there was no verification from the mobile companies as to in whose names such SIMs were issued nor were the persons in whose names such SIMs were issued were interrogated by the Investigating Officer.
  - "Besides above, another strong piece of evidence against the appellants was the record of mobile Sims collected from the Mobilink Company during investigation. Per prosecution case, the Investigating Officer provided IMEI number of robbed mobile phone to Mobilink Company, who informed the Investigating Officer that three SIMs vis. 0300-8934530, 0300-2387450 and 0308-2578199 were used in the said mobile after the incident, two SIMs were issued in the name of Muhammad Naseer Khan. On such information of Mobilink Company, the Investigating Officer remained in search of Muhammad Naseer Khan and on receiving credible information regarding the presence of Muhammad Naseer Khan along with his companions at Abdullah Shah Ghazi Chowrangi, arrested both the appellants and recovered some robbed articles. The prosecution also examined Atiqur Rehman, Co-Coordinator of Mobilink Company, who has supported the prosecution and produced the record of SIMs used in mobile phone robbed from the house of Imtiaz Khan. The record of mobile company and evidence of its representative is admissible in terms of Article 164 of Qanun-e-Shahadat Order which provides that the court may allow the production of any evidence that may have become available because of modern devices and techniques."

---

91 Salman Alias Lamba and Another vs. The State, 2018 YLR 1092 KHC
92 Kashif Ansar v. Aga Khan University, YLR 2013 KHC 2284.
D2.1.2.: Record from Social Media Companies

1. **Evidentiary Value and Relevancy**
   - See D1, except for provisions that apply specifically in the context of the IFTA, Section 19-C of the ATA and Section 9-A of the AMLA.

2. **General Guidelines**
   - For Guidelines on Transport of Evidence, see relevant sub-heading namely “Guidelines for Transport of Evidence” in Guidelines Code C.
   - See Guidelines on D2.1.1. with respect to Section 21EE of ATA, Section 25 of AMLA and Section 94 of CrPC.
     - At the time of receiving of information from concerned authorities, an expert on cyber/forensics department/wing will decipher the evidence in a presentable form for presentation before the court.
     - Thereafter, the IO shall seize the record under seizure and record the statement of the expert officer and witnesses under Section 161 of the CrPC.
   - Alternatively, when the IO requires assistance from an entity outside the jurisdiction of Pakistan, he may rely upon the Mutual Legal Assistance framework. This framework designates the Ministry of Interior as the designated authority for transmitting such requests. After such assistance has been received, the process of admissibility and evidentiary value will be as per the QSO.

D2.2: Audio/Video Recordings

1. **Evidentiary Value and Relevancy**
   - See D1, except for provisions that apply specifically in the context of the IFTA, Section 19-C of the ATA and Section 9-A of the AMLA.
   - The Supreme Court of Pakistan has laid down comprehensive guidelines with respect to audio/video recordings. A condensed version of the guidelines is as follows:
     - No audio tape or video can be relied upon by a court until the same is proved to be genuine and not tampered with or doctored. A forensic report prepared by an analyst of the Punjab Forensic Science Agency in respect of an audio tape or video is per se admissible in evidence in view of the provisions of section 9(3) of the Punjab Forensic Science Agency Act, 2007.
     - An audio tape or video sought to be produced in evidence must be the actual record of the conversation as and when it was made or of the event as and when it took place.
     - The person recording the conversation or event must be produced and must produce the audio tape or video. The audio tape or video must be played in the court, and ought to be clearly audible or viewable.
     - Any other person present at the time of making of the conversation or taking place of the event may also testify in support of the conversation heard in the audio tape or the event shown in the video.
     - The voices recorded or the persons shown must be properly identified.
     - The evidence sought to be produced through an audio tape or video must be relevant to the controversy and otherwise admissible.
     - Safe custody of the audio tape or video after its preparation till production before the court must be proved.
     - The transcript of the audio tape or video must have been prepared under independent supervision and control.
     - The person recording an audio tape or video may be a person whose part of routine duties is recording of an audio tape or video and he should not be a person who has recorded the audio tape or video for the purpose of laying a trap to procure evidence.

2. **General Guidelines**
   - For Guidelines on Transport of Evidence, see relevant sub-heading namely “Guidelines for Transport of Evidence” in Guidelines Code C.

---

93 Mutual Legal Assistance (Criminal Matters) Act, 2020
94 Ishtiaq Ahmed Mirza v. Federation of Pakistan, PLD 2019 SC 675; The unabridged guidelines have been attached as an addendum at the end of Guideline E.
• *Tahir Ahmed Naseem v. The State.* The bail petition showed the use of specialized agencies to confirm the alleged complaint or FIR that had been lodged against the accused and to subsequently utilize it within the trial. The accused was charged under ss. 153A, 295A-C and 298 of the Pakistan Penal Code, 1860. The accused and the complainant met on Facebook and, subsequently, met face to face. During investigation, the local Police took into custody audio recordings and oral statements in the form of a USB and his personal computer. The said content was also viral on the internet through the account of the accused. The pieces of evidence were dispatched to the Forensic Science Laboratory where they were analyzed through Forensic Tools and a Spectrographic test. The report of the Examiner, Digital Forensic/Audio Video Section, in Peshawar came in the affirmative.

**D3: ADDITIONAL GUIDELINES ON DIGITAL FORENSICS AND EVIDENCE**

**Recovering Data**
- Deleted files and other data that has not been overwritten
- Temporary auto-save files
- Print-spool files
- Websites visited, even where the browser history and cache have been deleted
- Communications sent via chat or IM
- Financial-based Internet transactions
- Documents, letters, and images created, modified, or accessed on the computer
- The time and date information about files

**Volatility of Digital Evidence**
- Digital evidence is more volatile than paper information; therefore, it can be easily altered or destroyed.
- Integrity must be preserved.
- If files are destroyed, it can give rise to a claim of spoliation of evidence.
- If authenticity is not supported or proven, evidence will be inadmissible.
- Rules regarding admissibility of digital evidence in court are the same.
- Types of Computer System Files

**Places to Search for Digital Evidence**
- Printers
- Internal hard drives
- Copiers and Scanners and multifunction devices
- Internal storage
- Fax machines
- Backup storage devices
- Removable storage
- Smartphones
- Cloud environments

**Privacy Issues**
Search policy should include personal electronic devices:
- Smartphones
- USB flash drives
- MP3 players
- Laptops

---

Computer Forensics Investigation Phases

Digital forensics typically involve these phases:

- Planning
- Seizing
- Imaging
- Analyzing
- Reporting and testifying

**Planning**
- Determine whether there are any privacy issues in the item(s) to be searched
- Make appropriate preparations if the investigation involves the use of a legal order.
- Ensure that all equipment used in a forensic capacity is legitimate and reliable.
- Ensure that the fraud examiner is properly trained to employ relevant digital forensic tools and that equipment is employed in the manner for which it was designed.

**Seizing**
- Involves ensuring that all relevant evidence is seized and secured in a forensically sound manner so that the evidence is not tainted or destroyed.
- Document the scene with photographs or a diagram.
- Look around for notes that might appear to be passwords, since many people write down or record their passwords near their computers.
- If the computer is off, leave it off.
- Collect volatile data “live” if required.
- Some data may be lost if the machine is shut down.
- Data can be collected while the machine is still on.
- If the computer is on, do not turn the system off using normal shutdown routines.
- Do not peek through the files.

**Imaging**
- Image acquisition involves using a standalone hard drive duplicator or similar device to duplicate a computer’s entire drive without altering it.
- This process is known as imaging because it takes a hard drive and images it to another hard disk drive or other media.
- Steps
  - Acquire the original storage media.
  - Create forensic image of the original media.
  - Verify the image of the original storage media.

**Processing**
- Involves processing and filtering digital information to reduce the amount of data that has been collected by identifying relevant information and by setting aside duplicates and other information that is not relevant due to its type, origin or date.
- Methods for filtering large amounts of data
  - Keyword searches
  - Deduplication filtering
  - Date range filtering
  - File type filtering

**Analyzing**
- Involves the use of specialized software designed to identify, extract, collect, examine and store digital artifacts.
- Best to use a combination of various forensic tools during the analysis phase.
Fraud examiners should look for inculpatory evidence (i.e., evidence that serves to incriminate the subject of the investigation) and exculpatory evidence (i.e., evidence that serves to disprove the subject’s involvement in the misconduct).

The primary concern is to maintain the integrity of the data at all times.

[For Guidelines on Transport of Evidence, see relevant sub-heading namely “Guidelines for Transport of Evidence” in Guidelines Code C.]

D4: FORENSICS: FINGERPRINTS AND HANDWRITING

1. Evidentiary Value and Relevancy
   - Opinion of Experts: All evidence found under Guidelines Code D must be proven through opinion of experts. The same is governed by Art. 59 of the QSO. The provision reads as follows:
     - When the Court has to form an opinion upon a point of foreign law, or of science/or art, as to identity of handwriting or finger impressions or as to authenticity and integrity of electronic documents made by or through an information system, the opinions upon that point of persons specially skilled in such foreign law science or art, or in questions as to identity of handwriting or finger impressions or as to the functioning, specifications, programming and operations of information systems, are relevant facts.

2. General Guidelines
   - For Guidelines on Transport of Evidence, see relevant sub-heading namely “Guidelines for Transport of Evidence” in Guidelines Code C.
   - Procedure for obtaining Expert Opinion on Handwriting:
     - When a document is in question (signatures / handwriting) in an investigation, it needs to be seized under a seizure memo.
     - Per Article 78 of the QSO, if a document is alleged to be signed by any person, the signature or the handwriting must be so proved to be him.
     - I.O. shall send this sealed envelope along with following covering letter.
     - It can be sent through courier or by hand.
     - It shall be sent to National Forensic Science Authority, H-11, Islamabad. [It shall be sent to a concerned forensic authority]
     - Custody form and other formalities guidelines can be found at https://www.nfsa.gov.pk/
     - Although there is no hard and fast rule as to the weight given to an expert, such reports are nonetheless not immune from judicial scrutiny.96

GUIDELINES CODE: E

ADDITIONAL EVIDENCE CONCERNING RELATIONSHIP WITH PROScriBED ORGANIZATIONS
<table>
<thead>
<tr>
<th>1. Evidentiary Value and Relevancy of Additional Evidence</th>
<th>115</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. General Guidelines</td>
<td>115</td>
</tr>
<tr>
<td>a. Overview</td>
<td>115</td>
</tr>
<tr>
<td>b. Appropriate Measures and Practices</td>
<td>116</td>
</tr>
<tr>
<td>c. Practices to Avoid</td>
<td>118</td>
</tr>
<tr>
<td>d. Protocols for Physical Evidence</td>
<td>118</td>
</tr>
<tr>
<td>e. Jurisprudence</td>
<td>119</td>
</tr>
</tbody>
</table>
There are certain pieces of evidence which can be used to link the accused to the proscribed organization and these include, but are not limited to:

- Pamphlets;
- Receipt books;
- Writing Instruments;
- Loudspeakers;
- Skin Hides etc. for the collection of donations.

1. Evidentiary Value and Relevancy
   - As per Section 2 (c) of the QSO, “evidence” includes:
     - all statements which the Court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry; such statements are called oral evidence; and
     - all documents produced for the inspection of the Court; such documents are called documentary evidence.

   Pamphlets, receipt books, writing instruments can be classified as documentary evidence under the domestic legal framework. Examples of documentary evidence can include photographs or, in a terrorism financing case, can also include the publications, literature or any other material being used by the proscribed entity/ individual to commit acts mentioned under Section 11F, H-J of the ATA 1997.

   Documentary evidence is required to be proved in accordance with the provisions of QSO. A document, unless proved and exhibited at the trial in accordance with law cannot be termed as evidence. The investigation officer has to take such evidence into possession for it to be used as prosecution evidence.

   Pertaining to the other evidence, which can help establish the relationship of the accused with a proscribed organization, such as physical evidence (objects), like loudspeakers, collection of skin hides etc. is classified as circumstantial evidence under the legal framework, which can be used to corroborate or support other direct evidence. All facts, except the contents of documents, may be proved by oral evidence. Therefore, such evidence must be exhibited and the testimony of witnesses can be used to admit such evidence.

   Article 164 read with Article 59 of the QSO allows modern forensic science to enter courts through the credible and valued scientific opinions of experts as evidence, in order to arrive at the truth. The testimony of a skilled witness is an important source of circumstantial evidence which is admissible under Article 59 of QSO. Furthermore, Section 510 CrPC allows reports of certain listed experts to be admitted into evidence.

   The knowledge, intent or purpose behind an offence if not proved through oral or documentary evidence may be proved through inference drawn from facts/circumstances of each case in accordance with rules regarding relevancy of facts provided in the Qanun-e-Shahadat Order, 1984.

2. General Guidelines
   a. Overview
      - For Guidelines on Transport of Evidence, see relevant sub-heading namely “Guidelines for Transport of Evidence” in Guidelines Code C.

      Before establishing the accused’s relationship with the proscribed organization, the prosecutor must prove that the organization is a proscribed organization.
      - This proof must be given by the Investigating Officer and presented by the prosecutor.
      - The failure to do so would help the accused since he would take the benefit of Article 129, QSO, illustration (g) of which states that evidence which could be but is not produced would, if produced, be unfavourable to the person who withholds it.
The primary evidence is the government notification that states that it is a proscribed organization. The Investigating Officer must obtain a certified copy of the notification from the concerned department or the Home Department, or the IO should obtain the document and verify it by writing through a written letter to the Home Department. A copy of the said letter should be available on the police record.

The statement of whoever applies for the notification, and collects it, and hands it over to the IO would also be included as part of evidence.

- Material piece of evidence is required regarding the activity of the accused (e.g. collection of funds or dissemination). Evidence for this would be the true account of that activity as a statement.
- Substantial pieces of evidence are necessary for the conviction of the accused. To establish the relationship of the accused with the proscribed organization, substantial evidence would include information about visits of the accused to the organization, call data records of the accused calling individuals from the organization, membership cards, and membership forms.
- Corroborative evidence would be required to support the material piece of evidence. This would include recovered material through seizures, including but not limited to the following:
  - Pamphlets;
  - Receipt books;
  - Writing Instruments;
  - Loudspeakers;
  - Donation boxes;
  - Skin Hides etc. for the collection of donations.
- Any recovered material, once sealed, must have an embossed mark on them, and the Investigating Officer’s name’s first initial must be written on it.
- Statements of individuals in tanneries who receive skin hides may also be relevant in establishing the connection of the accused to the proscribed organization.
- There are different laws on how to preserve perishable and non-perishable items, and for those that must be sent for examination by forensic labs, and those that must be preserved as they are recovered. The primary rule common to all forms of recovered material include the following:
  - From the place of recovery to the maalkhana police station, and from maalkhana to forensic labs (if any), and from forensic labs to maalkhana to court, the chain of custody must be established through oral evidence. The persons who delivered the evidence from one place to another must give statements under 161 CrPC which would be evidence of the chain of custody.
  - The recovered/sealed material should be transported under a legal cover, i.e. Road Certificate, which is usually obtained from the head of the police of the concerned district.
  - Prior to the transportation of the recovered material, its entry should be incorporated in all relevant registers.

b. Appropriate Measures and Practices

- Documentary evidence in the form of pamphlets, receipt books, writing instruments should be collected by following these guidelines:

<table>
<thead>
<tr>
<th>SR.</th>
<th>APPROPRIATE MEASURES</th>
<th>REASONS FOR APPROPRIATE MEASURES</th>
<th>ADDITIONAL COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Do not mark the document.</td>
<td>Markings destroy some of the identifying evidence originally present in the document for example, the investigating officer may underline a text for emphasis. This may be confused with similar marks made by the accused in the document.</td>
<td>Investigating officers should not write upon any documentary evidence except possibly as a means of subsequent identification of the document. In such cases the identification marks should be restricted to initials or numbers.</td>
</tr>
<tr>
<td>2.</td>
<td>Do not write upon documents.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td>Do not use pencils, pens, dividers, or erasers as pointers.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
If these marks are placed on a document which later is to be introduced as court evidence, the fact that the document is marked might, in some instances, prevent or hinder its admission in the court.

The ideal envelope or covering should be heavy weight, transparent, and made of cellophane. Documents to be filed should always be unfolded and placed in protective envelopes or folders and should be clearly marked so that the contents are easy to decipher.

4. Keep documents in envelopes or protective folders
   This is important to prevent contamination of the document. Folding the document may cause the ink on it to smudge or cause a crease in the document making the writing illegible. Furthermore, a fold can also lead to a tear in the document.
   The possible effects of moisture and heat should always be given special consideration whenever an investigator is storing documents for some length of time. Storage spaces that are unusually damp or warm should not be used.

5. Keep dry and away from excessive heat and strong light.
   This is important as exposure to heat and strong light may cause alterations or changes to the documents.
   The possible effects of moisture and heat should always be given special consideration whenever an investigator is storing documents for some length of time. Storage spaces that are unusually damp or warm should not be used.

6. Take documents to laboratory or an expert without delay.
   This is important because the document should be examined in its most original state as soon as possible.
   If an anonymous letter or a piece of writing is found with fingerprints, the document ought to be brought to the laboratory unopened. Moreover, a copy of the document may be made for purposes of further investigation. Latent fingerprints on paper become indistinct or disappear entirely within a very short time, hence, evidence should be brought to the laboratory immediately upon receipt.
c. Practices to Avoid

<table>
<thead>
<tr>
<th>SR.</th>
<th>PRACTICES TO AVOID</th>
<th>ADDITIONAL COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Do not mutilate by squeezing, repeatedly folding, cutting, or tearing.</td>
<td>Additional Comments</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Documents which are subject to laboratory examination should not be creased or folded.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If a document is subject to a tear, the investigator should not attempt to mend it himself, but should let the laboratory examiner repair it. Under no conditions should a document be pasted on another sheet of paper or cardboard in order to repair a tear or to strengthen a fold.</td>
</tr>
<tr>
<td>2.</td>
<td>Do not carry the document in a pocket for a prolonged period of time/ make copies of the documents for referral and subsequent usage.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Documents that are carried in the investigator’s pocket often become worn, frayed, and dirty leading to mild destruction of evidence.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Since Art. 76 of QSO allows admissibility of secondary documents, it is strongly recommended that copies of the primary document are made if the investigation is subject to extension. Officers should file or store documents at their headquarters if the documents are not needed during the investigation.</td>
</tr>
</tbody>
</table>

- These rules are primarily intended for the handling of questioned documents, such as handwritten or typewritten material about which there is some question concerning the author or manner of execution. However, they apply equally well to the preservation of specimens which are to be used for standards in handwriting and typewriting comparisons (i.e., specimens of handwriting or typewriting, the authorship of which is already established or admitted). In fact, any piece of handwriting, typewriting, or printing which might conceivably form a link in the chain of circumstantial evidence surrounding an investigation should be given the same care as documents whose importance is already known and recognized.

d. Protocols for Physical Evidence including loudspeakers, hides of animals etc.

- Once the physical evidence is recovered, all the relevant pieces of evidence are taken into safe custody by the Investigation Officers and trace evidence is dispatched on priority basis to the forensic laboratory. Any undue delay in the dispatch of evidence could diminish the legal value of the evidence. Additionally, any compromise in the chain of custody can make the evidence untrustworthy.

- Every piece of collected evidence has to be sealed and stamped at the crime scene and then sent to the forensics laboratory for examination (if needed). In practice, experienced IOs sequence their actions by keeping in view the legal requirements and by using their experience of presenting material in a trial. There have also been cases where IOs have used practices that have not been supported by law and which have created dents in the case of the
prosecution. According to Kareem Bukhsh vs. The State, “… the investigating Officer in order to establish the charge against the accused of firing should have sealed the recovered Kalashnikov at the spot and should have dispatched the recovered Kalashnikov along with the empties to the Forensic Expert to establish that the recovered weapons were functional or that such empties matched with the recovered weapons, but no such evidence was collected or dispatched, rendering the case of prosecution as doubtful.”

- Every activity of evidence collection and preservation is to be documented and entries in different registers of the police station are to be made to keep the evidence legally reliable and admissible.

e. Jurisprudence

- Section 9 of the Anti-Terrorism Act 1997 (ATA) unambiguously suggests that possession of inflammatory material by itself is an offence even before such material is distributed. If the accused is arrested red-handed, objection over non association of public witnesses to confirm the possession does not hold water either. Police officials, being functionaries of the state, are no less credible witnesses to drive home the charge. The officials who testified in the witness box had seemingly no axe to grind. In Qari Muhammad Ishaq Ghazi v. The State, it was held that police officials are as good witnesses as any other and their evidence is subject to same standard of proof and principles of scrutiny as applicable to other categories of witnesses, in the absence of any animus, infirmity, or flaw in their depositions, their statements can be relied without demur.

- In Abdul Hadi v. the State, there was an allegation against the accused that certain pamphlets were recovered from him. However, nothing was placed on record to show that either the police party saw the accused while distributing such material or even heard conversation of accused which could establish his link with such proscribed organization. No private person had been examined by the investigating officer with regard to distributing pamphlets to incite hatred or giving projection to any person convicted for a terrorist act or any proscribed organization.

- In the State v. Hafiz Muhammad Iqbal, the accused was charged for the offences of collecting funds for, and being affiliated with, a proscribed organization under Section 11F(2) and 11N of the ATA. A subscription book, which related to the collection of funds, was found to be filled with the handwriting of the accused, which was then used by the Prosecution to secure a conviction.

- In the State v. Muhammad Bilal Makki, the accused was raising funds for Jaish-e-Muhammad, as well as distributing books, in order to stir up sectarian violence and hatred. The accused was charged under Sections. 11F(5), 11-H, 11-I, 11-J, 11-N and Section 8-9 of the ATA. When the accused was raided, a receipt book of funds and collected money were recovered from him. Specifically, within the receipt book, out of serial Nos. 151 to 185, Nos. 151 to 167 were cut off and had signatures of the accused. To this end, the prosecution relied upon police witnesses and the items themselves. In response, defence counsel argued that the receipt book contained no information of any donors. On a totality of evidence, as well as the testimonies of prosecution witnesses, the Court was able to find the accused guilty. In turn, this case demonstrates how primary evidence was utilized and linked to one another so as to form a coherent narrative which was then able to secure a conviction for TF.

105 Interview with prosecutor, (Islamabad, 25 May 2017). Note: Such practices not only contaminate the evidence, but also cause delays in investigation during which time the accused is held in custody, even if innocent. Moreover, evidence is routinely tampered with. For instance, empties have to be submitted into evidence even before the recovery of the gun. However, this is not the practice. Everything is recovered and placed together in evidence thereby breaking the chain of custody of evidence or raising doubts as to the credibility of the empties being fired from the gun in the commission of the crime or later on by the police just to show recovery of empties.

106 Kareem Bukhsh v. The State, 2017 YLR 1779

107 Qari Muhammad Ishaq Ghazi v. The State, 2019 SCMR 1646

108 Abdul Hadi v. The State, 2016 PCRLJ Note 70.
ANNEXURES
## IN THIS SECTION

1. **Annexure I: Templates for Witness Statements:**
   - Template to Record Statement under Section 161, CrPC. (123)
   - Template to Require Attendance at Investigations (124)

2. **Annexure II: Templates to Obtain Financial Records:**
   - Template for Application to the Court for Want of Bank Record (125)
   - Template for Letter to Bank for Want of Record (126)
   - Template for Letter to all Banks to Identify Bank Accounts (128)
   - Template of Letter to Obtain Record of Income Tax etc. from FBR (130)
   - Template of Letter to Obtain Record from Excise Department (131)
   - Template of Letter to Obtain Record of Immoveable Properties (132)
   - Template of Letter to Obtain Record of NPOs (133)
   - Template of Letter to Obtain Records from NADRA (134)
   - Template of Letter to Obtain Records from DG-IMPASS (135)
   - Template of Letter to Obtain Records from FIA- Integrated Border Management System (IBMS) (136)

3. **Annexure III: Templates for Expert Analysis and Findings**
   - Template of Letter to Obtain Call Detail Records (CDR), etc. (137)
   - Template of Letter to Obtain Forensic Analysis of Digital Equipment (138)
   - Template for Application to Court for Social Media Applications Record (140)
   - Template of Letter to Obtain Record from Social Media App Authorities etc. (141)
   - Template of Letter to Obtain Expert Opinion on Fingerprint and Handwriting. (142)
ANNEXURE I: TEMPLATES FOR WITNESS STATEMENTS

a. Template to Record Statement under Section 161, CrPC.

**STATEMENT UNDER SECTION 161 CRIMINAL PROCEDURE CODE**

FIR No. ____________ u/s ____________ Date ____________ u/s ____________

Police State __________________________ District __________________________

Witness __________________________ s/o __________________________

Caste __________________________

Was examined in the subject case who stated as under:

**STATEMENT**

________________________________________

________________________________________

________________________________________

________________________________________

________________________________________

________________________________________

________________________________________

________________________________________

Date: __________________________

________________________________________

Signature of the Police Officer
b. Template to Require Attendance at Investigations.

**FORM 25.2(1) Police Rules**

**ORDER TO REQUIRE ATTENDANCE AT INVESTIGATIONS UNDER SECTIONS 160 AND 175, CRIMINAL PROCEDURE CODE**

<table>
<thead>
<tr>
<th>Name</th>
<th>S/o</th>
<th>Caste</th>
<th>Resident of</th>
</tr>
</thead>
</table>

Whereas the presence of the aforesaid person is necessary for the purpose of enquiry into the offence reported to have been committed under section _____________ at the Police Station ______________; therefore, the said persons is hereby directed to appear before the undersigned at (place) ____________ on (date) ______________ at (hour) _______________ to give such information in relation to the said alleged offence as he may possess.

__________________________
Signature and Designation of the Issuing Police Officer

Date:_______________________

Hour:_______________________

(Name) __________________ mentioned in this order attended on (date) ______________ at (hour)_______

at (place) __________________ and was permitted to leave on (date) ______________ at

(hour)____________________ at (place) ________________________________.

Dated: _______________________

__________________________
Signature and Designation of the Issuing Police Officer

**Note:** Summons/Warrants can be served through post/by process server, and an endorsement on the back of a duplicate copy of the summons is mandatory.
ANNEXURE II: TEMPLATES TO OBTAIN FINANCIAL RECORDS

a. Template for Application to the Court for Want of Bank Record.

Subject: Application to obtain bank record in case FIR No. _____ dated _____ under Section _____ of Police Station______.

Respectfully submitted that:

Subject Case was registered against (Accused’s Name and CNIC, Father’s Name, Address) upon allegations of (brief facts of the case). During the course of investigation, it transpired that the following bank account(s) is/are involved/used in commission of crime:

Title of Account: _______________________

Account Number: _______________________

Bank Branch: _________________________

Undersigned has reasonable cause to believe that from record(s) of the aforementioned bank account(s), sufficient incriminating evidence can be obtained which will be helpful in the conclusion of investigation. Therefore, it is requested that the application may kindly be allowed with a direction to the concerned bank authorities to provide the requisite record in connection with the bank account(s) mentioned above.

(Signed)
Name and Designation of Investigation Officer
Police Station
Date

Forwarded by Legal Officer
b. Template for Letter to Bank for Want of Record.

Departmental Letterhead

Reference No.______________ Date: ______________

The Branch Manager,
Bank Name
Branch Name & Address

Subject: Request for Provision of Record u/s (94 CrPC. / 21EE ATA / 25(1) AMLA) in case FIR No. ______ dated _____ under Section ______ of Police Station ______.

Reference as above.

1. Subject Case was registered against (Accused’s Name and CNIC, Father’s Name, Address) upon allegations of (brief facts of the case).

2. During the course of investigation, it transpired that the following bank account(s) is/are involved in the commission of crime:

   Title of Account: __________________________
   Account Number: __________________________
   Bank Branch: ______________________________

3. Undersigned has reasonable cause to believe that from the record(s) of the aforementioned bank account(s), sufficient incriminating evidence can be obtained, which will be helpful in the conclusion of investigation.

4. In view of the above, it is requested that the following attested record of bank account mentioned in para 2 may please be provided at the earliest for completion of investigation:
   - Account Opening Form
   - KYC
   - Specimen Signature Card
   - Bank Statements

The aforementioned detail may also be formatted as per following table:

<table>
<thead>
<tr>
<th>A/C Number</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A/C Title</td>
<td></td>
</tr>
<tr>
<td>Date of Account opening</td>
<td></td>
</tr>
<tr>
<td>Nature of Account</td>
<td></td>
</tr>
<tr>
<td>Nature of Business / source of income</td>
<td></td>
</tr>
<tr>
<td>Address(s) of Account holder and businesses</td>
<td></td>
</tr>
<tr>
<td>Turnover</td>
<td></td>
</tr>
<tr>
<td>Name of Signatories</td>
<td></td>
</tr>
</tbody>
</table>
### ANNEXURES

<table>
<thead>
<tr>
<th>Name of Branch</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact No.(s) Branch</td>
<td></td>
</tr>
<tr>
<td>Particulars and contact number of concerned bank officials including branch manager and operation manager</td>
<td></td>
</tr>
<tr>
<td>Total No. of Debit Transaction</td>
<td></td>
</tr>
<tr>
<td>Total No. of Credit Transaction</td>
<td></td>
</tr>
<tr>
<td>Total no. of Cash transactions and volume</td>
<td></td>
</tr>
<tr>
<td>Credit vouchers and detail of counter parties</td>
<td></td>
</tr>
<tr>
<td>Debit vouchers and detail of counter parties</td>
<td></td>
</tr>
<tr>
<td>Cheques withdrawal detail</td>
<td></td>
</tr>
<tr>
<td>Inter-bank transfer detail</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>S No.</th>
<th>Date</th>
<th>Debit Amount</th>
<th>A/C No.</th>
<th>A/C Title and Account holder name</th>
<th>Bank with Branch name</th>
<th>Name</th>
<th>CNIC</th>
<th>Contact No./Mobile No.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>S No.</th>
<th>Date</th>
<th>Credit Amount</th>
<th>A/C No.</th>
<th>A/C Title and Account holder name</th>
<th>Bank with Branch name</th>
<th>Name</th>
<th>CNIC</th>
<th>Contact No./Mobile No.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Soft copy of the data may also be provided.

5. It is also requested that a focal officer from your bank may please be informed and be directed to contact the undersigned for further coordination and assistance.

**Enclosure:**
Court permission u/s 94 CrPC. 1898

(Signed)
Name & Designation of I.O.
Police Station
Date
c. Template for Letter to all Banks to Identify Bank Accounts.
(No Court Permission Required)

Departmental Letterhead

**Subject:** Request for Provision of Record u/s (94 CrPC. / 21EE ATA / 25(1) AMLA) in case FIR No. ______ dated ______ under Section ______ of Police Station ______.

1. Subject Case was registered against (Accused's Name and CNIC, Father’s Name, Address) upon allegations of (brief facts of the case).
2. During the course of investigation, it transpired that the said accused is maintaining multiple bank accounts in different banks in furtherance of the commission of the offence under investigation with this police station.
3. In view of the above, it is requested that this office may please be intimated if your bank is maintaining bank account(s) in any branch against the CNIC of the said accused. Your cooperation will be appreciated.

(Signed)
Name & Designation of I.O.
Police Station
Date

Reference No. ______ dated: ______

1. **President**, First Women Bank Limited, Dr. Syedna Tahir Saifuddin Memorial Foundation Building, CL-10/20/2, Beaumont Road, Civil Lines, **Karachi**
2. **President**, Sindh Bank Limited, 3rd Floor, Federation House, Abdullah Shah Ghazi Road, Clifton, **Karachi**
3. **President**, The Bank of Punjab, Head Office, BOP TOWER, 10-B, Block E-11, Main Boulevard Gulberg-III, **Lahore**
4. **President**, National Bank of Pakistan, Head Office, I.I. Chundrigar Road, **Karachi**
5. **Acting Managing Director**, The Bank of Khyber, 24- The Mall, Head Office, Peshawar Cantt, **Peshawar**
6. **Acting Managing Director**, Industrial Development Bank Limited, State Life Building No. 2, Wallace Road, Off. I. I. Chundrigar Road, **Karachi**
7. **Acting Chief Executive Officer**, The Punjab Provincial Cooperative Bank Ltd, Head Office, Bank Square, Shahrah-e-Quaid-e-Azam, The Mall, **Lahore**
8. **President / Chief Executive Officer**, SME Bank Limited, 56-F, Nazim-ud-Din Road, F-6/1, Blue Area, **Islamabad**
9. **President / Chief Executive Officer**, Zarai Taraqiati Bank Limited, Head Office, 1-Faisal Avenue, Zero Point, **Islamabad**
10. **Chief Executive Officer**, Allied Bank Limited, Head Office and Registered Office, 3 Tipu Block, Main Boulevard, New Garden Town, **Lahore**.
11. **President/Chief Executive Officer**, Bank Alfalah Limited, Head Office, 2nd Floor, B.A. Building, I.I. Chundrigar Road, **Karachi**
12. **President/ CEO**, Faysal Bank Limited, Faysal Bank Limited, Faysal House, 4th Floor, St-02, Commercial Lane, Main Shahrah-e-Faisal, **Karachi**
13. **President/ CEO**, Habib Metropolitan Bank Limited, President Office, Spencer building, Mezzanine floor, I.I. Chundrigar Road, **Karachi**.
14. **President/Chief Executive**, MCB Bank Limited, 22nd Floor, MCB Tower, I.I. Chundrigar Road, **Karachi**. 9th Floor, MCB House, 15-Main Gulberg, **Lahore**.
15. **President / Chief Executive Officer**, SILK BANK Limited, 22nd Floor, Centre point, Near KPT Interchange, Korangi, Karachi. 6-Q Block, Gulberg II, Lahore

16. **President / Chief Executive Officer**, Standard Chartered Bank (Pakistan) Limited, 3rd Floor, Main Building, P.O. Box No. 5556, I.I. Chundrigar Road, Karachi

17. **President/Chief Executive Officer**, United Bank Limited, 21st Floor, UBL Head Office, I.I. Chundrigar Road, Karachi

18. **Acting President/Chief Executive Officer**, Askari Bank Limited, 3rd Floor, Plot No.18, NPT Building, F-8 Markaz, Islamabad.

19. **Chief Executive/Managing Director**, Bank Al Habib Limited, MacKinnon Building I.I. Chundrigar Road, Karachi

20. **President/Chief Executive**, Habib Bank Limited, 22-Habib Bank Plaza I.I. Chundrigar Road, Karachi

21. **President/ CEO**, JS Bank Limited, 1st Floor, Shaheen Commercial Complex Dr. Ziauddin Ahmed Road, Karachi

22. **President/Chief Executive**, SAMBA Bank Limited, 6th Floor, Sidco Avenue Centre, Maulana Deen Muhammad Wafai Road, Karachi

23. **President/Chief Executive Officer**, Soneri Bank Limited, Central Office, 10th floor, PNSC Building, M.T.Khan Road, Karachi


25. **President / Chief Executive Officer**, Al Baraka Bank (Pakistan) Limited4th floor, 162, Bangalore Town, Main Shahrah-e-Faisal, Karachi.

26. **President / Chief Executive**, Dubai Islamic Bank Pakistan Limited, Hassan Chambers, 3rd Floor, Plot DC-7, Block-7, Kehkashan Clifton, Karachi

27. **President/Chief Executive**, MCB Islamic Bank Limited, 1st Floor, 339-Z Block, Commercial Area, Phase-III, DHA, Lahore

28. **Chief Executive Officer**, BankIslami Pakistan Limited, 11th Floor, Executive Tower, Dolmen City Marine Drive, Block-4, Clifton, Karachi

29. **President & Chief Executive Officer**, Meezan Bank Limited, Meezan House, C-25, State Avenue, SITE, Karachi

30. **Managing Director & Country Officer**, Citibank N.A. - Pakistan Operations, 1st Floor, AWT Plaza, I.I. Chundrigar Road, Karachi

31. **Chief Executive Officer-Pakistan**, Industrial and Commercial Bank of China Limited - Pakistan Branches, 16th Floor, Ocean Tower,G-3 Block 9, Scheme No 5, Main Clifton Road, Karachi.

32. **Chief Executive Officer**, Bank of China Limited-Pakistan Operations, 5th Floor., Corporate Office Block Dolmen City, HC-3, Block 4, Scheme 5, Clifton, Karachi

33. **Managing Director & Chief Country Officer**, Deutsche Bank AG – Pakistan, Operations, Avari Plaza, Fatima Jinnah Road, Karachi-75530

34. **General Manager**, MUFG Bank Limited, 1st Floor, Shaheen Complex, M.R. Kayani Road, Karachi
d. Template of Letter to Obtain Record of Income Tax etc. from FBR.

---

**Departmental Letterhead**

Reference No. _______________  
Date: _______________

The Regional Commissioner  
RTO Region ______  
Address

**Subject:** Request for Provision of Record u/s (94 CrPC. / 21EE ATA / 25(1) AMLA) in case FIR No. ______ dated ______ under Section ______ of Police Station ______.

Reference as above.

1. Subject Case was registered against (Accused’s Name and CNIC, Father’s Name, Address) upon allegations of (brief facts of the case).

2. For the conclusion of investigation, we are required to match his official financial profile, declared through filing income tax returns and wealth statements, with his financial profile/transactions under investigation. Therefore, your office is requested to provide income tax returns and the wealth statement of the aforementioned accused from financial year ______ to date. The record provided by you will be used for investigation purposes and shall not be used in the Court as evidence.

   Your cooperation in this respect shall be highly appreciated.

(Signed)  
Name & Designation of I.O.  
Police Station

---
Departmental Letterhead

Reference No.______________ Date: ______________

The Excise and Taxation Officer
Region
Address

Subject: Request for Provision of Record u/s (94 CrPC. / 21EE ATA / 25(1) AMLA) in case FIR No. _______ dated _______ under Section _______ of Police Station _______.

Reference as above.

1. Subject Case was registered against (Accused’s Name and CNIC, Father’s Name, Address) upon allegations of (brief facts of the case).
2. During course of investigation, it transpired that there is a likelihood of concealment of facts by the accused person vis-à-vis his financial position and assets held thereof. To conclude financial investigation in the subject case, it is inevitable to unearth all assets, moveable and immoveable, of the accused. Therefore, your office is requested to provide details of the vehicle registered against the CNIC of the accused, if any

Your cooperation in this respect shall be highly appreciated.

(Signed)
Name & Designation of I.O.
Police Station
f. Template of Letter to Obtain Record of Immoveable Properties.

Departmental Letterhead

Reference No.______________ Date: ________________

The Deputy Commissioner
Name of the District

**Subject:** Request for Provision of Record u/s (94 CrPC. / 21EE ATA / 25(1) AMLA) in case FIR No. ______
dated ______ under Section ______ of Police Station ______.

Reference as above.

1. Subject Case was registered against (Accused’s Name and CNIC, Father’s Name, Address) upon allegations of
   (brief facts of the case).
2. During the course of investigation, it transpired that there is a likelihood of concealment of facts by the accused
   person vis-à-vis his financial position and assets held thereof. To conclude our financial investigation in the
   subject case, it is inevitable that we unearth all assets, moveable and immoveable, of the accused. Therefore, your
   office is requested to provide details of immoveable property against the CNIC of the accused, if any.

   Your cooperation in this respect shall be highly appreciated.

   (Signed)
   Name & Designation of I.O.
   Police Station
g. Template of Letter to Obtain Record of NPOs.

Departmental Letterhead

Reference No.______________  Date: ________________

The Registrar,
Name and Address of the Registration Authority

Subject: Request for Provision of Record u/s (94 CrPC. / 21EE ATA / 25(1) AMLA) in case FIR No. ______
dated ______ under Section ______ of Police Station ______.

Reference as above.

1. Subject Case was registered against (Accused’s Name and CNIC, Father’s Name, Address) upon allegations of
(brief facts of the case).
2. During the course of investigation, it transpired that there is a likelihood of misuse of an NPO namely _____
registered at your office, for the purpose of Money Laundering/Terrorism Financing (ML/TF) by the accused
person(s). Therefore, your office is requested to provide the following attested record of the NPO:
   • Registered name, registration no. and date of registration
   • Names, CNICs and contact numbers of trustees and office holders
   • Memorandum and articles of associations
   • Trust deed
   • Bank accounts
   • Assets declarations
   • Audit reports from ___ to date
   • Detail of penalties with reasons, if any
   • Anomalies/shortcomings identified, if any
   • Any other relevant record

   Your cooperation in this respect shall be highly appreciated.

(Signed)
Name & Designation of I.O.
Police Station
h. Template of Letter to Obtain Records from NADRA.

```
Departmental Letterhead

Reference No.______________ Date: ________________

The CoS to Chairman
NADRA Headquarters
Islamabad

Subject: Request for Provision of Record u/s (94 CrPC. / 21EE ATA / 25(1) AMLA) in case FIR No. ______ dated ______ under Section ______ of Police Station ______.

Reference as above.

1. Subject Case was registered against (Accused’s Name and CNIC, Father’s Name, Address) upon allegations of (brief facts of the case).

2. Your office is requested to provide verisys and family tree (by birth and by marriage) of CNIC No. ________________, which is urgently required to proceed further into the investigation.

   Your cooperation in this respect shall be highly appreciated.

(Signed)
Name & Designation of I.O.
Police Station
```
i. Template of Letter to Obtain Records from DG-IMPASS.

**Departmental Letterhead**

Reference No._____________ Date: _______________

The Director General  
IMPASS  
G-8/1, Islamabad

**Subject:** Request for Provision of Record u/s (94 CrPC. / 21EE ATA / 25(1) AMLA) in case FIR No. ______ dated ______ under Section ______ of Police Station ______.

Reference as above.

1. Subject Case was registered against (Name of Accused, Father’s Name, Address and CNIC) upon allegations of (brief facts of the case).
2. Your office is requested to provide KB-9 Form of CNIC No. ______________, which is urgently required to proceed further into the investigation.

Your cooperation in this respect shall be highly appreciated.

(Signed)

Name & Designation of I.O.  
Police Station
j. Template of Letter to Obtain Records from DG-IMPASS.

Departmental Letterhead

Reference No._______________ Date: _______________

The Director IBMS
FIA Headquarters
G-9/4, Islamabad

Subject: Request for Provision of Record u/s (94 CrPC. / 21EE ATA / 25(1) AMLA) in case FIR No. ______ dated ______ under Section ______ of Police Station ______.

Reference as above.

1. Subject Case was registered against (Name of Accused, Father’s Name, Address and CNIC) upon allegations of (brief facts of the case).
2. Your office is requested to provide the travel history of CNIC no. ________________, which is urgently required to proceed further into the investigation.

Your cooperation in this respect shall be highly appreciated.

(Signed)
Name & Designation of I.O.
Police Station
ANNEXURE III: TEMPLATES FOR EXPERT ANALYSIS AND FINDINGS

a. Template of Letter to Obtain Call Detail Records (CDR), etc.

Departmental Letterhead

Reference No. __________ Date: __________

The CoS to Chairman
PTA
G-8/4, Islamabad

Subject: Request for Provision of subscriber’s detail and CDR u/s (94 CrPC. / 21EE ATA / 25(1) AMLA) in case
FIR No. ______ dated ______ under Section ______ of Police Station ______.

Reference as above.

1. Subject Case was registered against (Accused’s Name and CNIC, Father’s Name, Address) upon allegations of
   (brief facts of the case).

2. During the course of investigation, it transpired that important incriminating evidence/further links of the
   accused can be found/traced through his Cell No. __________, retrieved from his cell phone seized in the
   subject case.

3. In view of the above, your office is requested to provide the subscriber’s detail and CDR against the cell number
   mentioned in Para-2 above, which is urgently required to proceed further into the investigation.

   Your cooperation in this respect shall be highly appreciated.

   (Signed)
   Name & Designation of I.O.
   Police Station
b. Template of Letter to Obtain Forensic Analysis of Digital Equipment.

Departmental Letterhead

Reference No. _______________ Date: _______________

The Director,
Cyber Crimes Wing,
2nd Floor, NPF Building,
G-10/4, Islamabad

Subject: Request for Provision of Technical Analysis Report u/s (94 CrPC. / 21EE ATA / 25(1) AMLA) in case
FIR No. ______ dated ______ under Section ______ of Police Station ______.

Reference as above.

1. Subject Case was registered against (Accused’s Name and CNIC, Father’s Name, Address) upon allegations of
(brief facts of the case)
2. During the course of investigation, it transpired that important incriminating evidence/further links of the
accused can be found/traced through digital equipment mentioned below seized in the subject case:

<table>
<thead>
<tr>
<th>S No.</th>
<th>Description of digital equipment</th>
<th>Made and model</th>
<th>IMEI No. / HDD serial no.</th>
</tr>
</thead>
</table>

3. In view of the above, your office is requested to provide a technical analysis report vis-à-vis the data retrieved
from the digital equipment mentioned in Para-2 above which is urgently required to proceed further into the
investigation.

Your cooperation in this respect shall be highly appreciated.

Enclosure: Form-31

(Signed)
Name & Designation of I.O.
Police Station

Form-31
Electronic Evidence Chain of Custody

<table>
<thead>
<tr>
<th>Laboratory Case File No.</th>
<th>Date &amp; Time of Receiving</th>
<th>29-June-2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of the Organization from which the equipment is received.</td>
<td>Name</td>
<td>(Name of IO)</td>
</tr>
<tr>
<td></td>
<td>Address</td>
<td>(Address of LEA)</td>
</tr>
<tr>
<td></td>
<td>Contact No.</td>
<td></td>
</tr>
<tr>
<td>Type of evidence to be required by the said organization</td>
<td>(Description of type of data required to be retrieved. It can be all data, partial data or data against some key words.)</td>
<td></td>
</tr>
</tbody>
</table>
## Detail of Electronic Equipment / Mobile phones Received

<table>
<thead>
<tr>
<th>S No.</th>
<th>Description of the Evidence</th>
<th>Serial No. / Model No. / IMEI</th>
<th>Brand / Manufacturer Name</th>
</tr>
</thead>
</table>

## Chain of Custody Log

<table>
<thead>
<tr>
<th>S No.</th>
<th>Received from</th>
<th>Received by</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Designation</td>
<td>Designation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date &amp; Time</td>
<td>Date &amp; Time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Signature</td>
<td>Signature</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
c. Template for Application to Court for Social Media Applications Record.

In the Court of Judicial Magistrate / ATC (address and city of the Court)

Subject: Application u/s 94 CrPC. / 21EE ATA for provision of information from Facebook authorities in case FIR No. ______ dated ______ under Section ______ of Police Station ______.

Respectfully submitted that:

1. Subject Case was registered against (Accused’s Name and CNIC, Father’s Name, Address) upon allegations of (brief facts of the case).
2. During the course of investigation, it transpired that important incriminating evidence/further links of the accused can be found/traced through his Facebook account ID: ____________, retrieved from his cell phone seized in the subject case.
3. In view of the above, it is prayed that the application may kindly be allowed with a direction to the concerned authorities to provide the requisite record in connection with the Facebook ID mentioned above.

(Signed)
Name & Designation of I.O.
Police Station
Date
d. Template of Letter to Obtain Record from Social Media App Authorities etc.

Departmental Letterhead

Reference No.______________  Date: ________________

The CoS to Chairman
PTA
G-8/4, Islamabad

Subject: Request for provision of information from Facebook authorities in case FIR No. ______ dated ______ under Section ______ of Police Station ______.

Reference as above.

1. Subject Case was registered against (Accused’s Name and CNIC, Father’s Name, Address) upon allegations of (brief facts of the case).
2. During the course of investigation, it transpired that important incriminating evidence/further links of the accused can be found/traced through his Facebook account ID: __________, retrieved from his cell phone seized in the subject case.
3. In view of the above, your office is requested to approach Facebook authorities to provide the following detail, which is urgently required to proceed further into the investigation:

   • Date of account opening
   • Detail/IDs of friends
   • Pages Liked through the said ID
   • Pages formed and contents of uploads with dates
   • Contents of posts created with dates
   • Contents of posts shared with dates
   • Content and date of post [some specific post under investigation]
     • IDs who liked this post
     • IDs who shared this post
     • IDs with contents of comments made

   Your cooperation in this respect shall be highly appreciated.

Enclosure: Court permission

(Signed)
Name & Designation of I.O.
Police Station
Departmental Letterhead

Reference No._________________________ Date: __________________

Subject: Request for forensic analysis of questioned document seized in case FIR No. ______ dated ______ under Section ______ of Police Station ______.

Reference as above.

1. Subject Case was registered against (Accused’s Name and CNIC, Father’s Name, Address) upon allegations of (brief facts of the case).
2. During the course of investigation, the questioned document was seized under seizure memo dated ________.

To reach a logical conclusion regarding the role of the alleged person mentioned in Para-1 above, it is inevitable that we ascertain the authenticity of the signature/handwriting on the questioned document.

3. In view of the above, your office is requested to provide an expert opinion/forensic analysis vis-à-vis the signature/handwriting on the questioned document after comparing it with the routine and specimen signature/handwriting documents (enclosed in a sealed envelope).

4. The matter is being referred to your office through (courier/by hand) and the undersigned affirms the custody of the said documents and handing them over to your office. The reply may please be provided through the same chain of custody.

Enclosure: Sealed envelope of the original questioned document, routine documents and specimen documents (page 1 to page _____)

(Signed)
Name & Designation of I.O.
Police Station
Contact No.

Evidence Receiving Unit, National Forensic Science Authority, H-11, Islamabad