Module 4

Planning Investigations: Investigation of Corruption and Money Laundering
(adopted from the Handbook for Practitioners on Asset Recovery under StAR Initiative)

The World Bank Group
## Contents

- Overview ................................................................................................................................................... 3
- Case Management/Division of responsibilities ......................................................................................... 4
- Initiating cases of corrupt practices and identifying money laundering activity ........................................... 5
- Creating a Subject Profile .......................................................................................................................... 6
- Avenues of Obtaining Financial Data and Other Evidence ........................................................................ 7
  - Information from Public Sources and Other Government Agencies ......................................................... 9
  - Other venues to Obtaining Financial Data and Other Evidence ................................................................. 12
- Interviewing targets and non-targets ........................................................................................................... 14
- Identifying Relevant Data: Examples from Commonly Sourced Documents ................................................. 15
  - Account Opening Documents and KYC/CDD Records ........................................................................... 15
  - Bank Account Statements ......................................................................................................................... 16
  - Wire Transfers ......................................................................................................................................... 17
  - Accounting Records ................................................................................................................................. 17
  - Purchase and Sale Documents .................................................................................................................. 18
  - Tracing assets (or managing evidence) ..................................................................................................... 18
- Summary and Review of Module 4 .............................................................................................................. 22
Overview
This module looks at the practical aspects of planning and management of investigations. It addresses the issue of initiating cases of corrupt practices and identifying money laundering activity. The module then goes on to explore the sources of information to facilitate an investigation; the use of investigation techniques; tracing assets and managing of evidence; as well as case management and division of responsibilities. Furthermore, various methods of gathering evidence such as surveillance, undercover operations, search warrants and informants, are explored. This module crystallizes the discussion had in module 1, 2 and 3 in so far as it deals with the matter of the management of an entire corruption investigation.

The module is a derivation of chapter 3 of the Handbook for Practitioners on Asset Recovery published by the Financial Market Integrity unit under the auspices of the Stolen Asset Recovery Initiative. As such, for a detailed discussion on issues related to the techniques that practitioners can use to trace assets and analyze financial data, as well as to secure reliable and admissible evidence for asset confiscation cases, reference should be made to this handbook. This module only covers some pertinent practical aspects of how to initiate, plan and manage corruption and money laundering cases.

At the end of the study of this module, practitioners are expected to:

- Know and grasp practical ways of managing complex corruption and money laundering cases including the art of the division of responsibilities;
- Learn the many sources of information available to enable practitioners conduct an effective and efficient corruption and money laundering investigations; and
- Learn how to identify relevant financial and other valuable data since numerous documents will surface throughout an investigation.
Case Management/Division of responsibilities
Successful investigation of corruption and money laundering requires a comprehensive plan of action that incorporates a number of important steps and considerations. Practitioners will need to gather and assess the facts in order to understand the case, assemble a team, identify key allies, and communicate with foreign counterparts.

A prosecutor should normally lead the investigation or follow investigations conducted by investigating judges or law enforcement as the prosecution is ultimately responsible for presenting the case to the court and must ensure that law enforcement agencies collect the necessary evidence to establish the offenses, provisional measures and confiscation.¹ In addition, the prosecutor acts as an interface with judges when investigators need judicial authorization to use special investigative tools, such as wire-tapping, searches, arrests and plea bargaining.

Particularly in large, complex cases, it will be important to assemble a multidisciplinary team or unit to ensure the effective handling of the case and eventual confiscation. This will likely include a range of practitioners, including financial investigators and experts in financial analysis, forensic accountants, law enforcement, prosecutors, and asset managers. Experts may be appointed from the private sector or seconded from other agencies (e.g., regulatory authority, FIU, tax authority, auditing agency or office of the inspector general). Depending on the jurisdiction and circumstances of the case, this will likely involve investigative² and prosecutorial teams and may expand to a joint task force of the relevant agencies or joint investigation with a foreign jurisdiction.

Investigative teams should include individuals with the expertise necessary to analyze significant volumes of financial, banking and accounting documents, including wire transfers, accounting or financial statements, tax or customs records. They should also include investigators with experience in gathering business and financial intelligence, identifying complex illegal schemes, following the money trail and using investigative techniques including electronic surveillance, wire-tapping, search warrants, and witness interviews. In some cases, it may be useful or necessary to appoint experts or consultants who bring technical expertise, for example in financial analysis, forensic accounting, and computer forensics.

¹ In some civil law jurisdictions, investigating magistrates may lead the investigations from the beginning of the case until its final adjudication; however prosecutors can appeal their decisions.
² “Investigative teams” includes investigations or intelligence gathering that takes place before and after the initiation of charges against the defendant. In some jurisdictions, the term “investigation” is used exclusively for investigations that follow the initiation of formal charges.
The law enforcement or prosecution agencies having primary responsibility for the specific offenses involved in the case often have the capacity to gather and present the evidence required for the purpose of confiscation. Where possible, there is also merit in creating specialized confiscation investigation and prosecution units to support primary criminal investigation teams. Experience suggests that it can be difficult when investigators and prosecutors are responsible for both the specific offense and the confiscation. In some jurisdictions, for example, criminal prosecutors are not assigned until the investigation is largely complete—which will be too late for the purposes of asset confiscation. In addition, investigators and prosecutors have large case-loads and tend to give priority to obtaining the criminal conviction, not necessarily the confiscation.

With the establishment of specialized confiscation units, investigators and prosecutors develop the specialized skills needed to present evidence effectively for the purpose of enforcing confiscation laws. Confiscation investigators will generally go further than criminal investigators in identifying and tracing assets for the purpose of confiscation and they are well-placed to undertake international enquiries to follow assets that have left the jurisdiction. If such an approach is taken, confiscation practitioners must work closely with their counterparts pursuing the criminal prosecution to ensure the two run in harmony.

The team may be based in anti-corruption agencies that have the authority to investigate or prosecute or both, or in regular law enforcement and prosecution agencies. Wherever it is situated, it will be critical that investigators and prosecutors are granted, in law, the authority to investigate and/or prosecute the offenses and confiscate the proceeds of those offenses.3

**Investigating money laundering activities**

One of the biggest challenges in a corruption/money laundering case is producing the evidence which links the assets to the criminal activities (property-based confiscation) or proving that assets are a benefit derived from an offence committed by the offender (value-based confiscation).4 To establish this link (also referred to as the “nexus” or a “paper trail”), practitioners must identify and trace assets or “follow the money” until the link with the offense or location of the assets can be determined.

Experience has demonstrated that it is important to trace assets at the early stages of an investigation simultaneously with the investigation into the predicate or money laundering offenses and that establishing a framework or investigative plan is an important first-step for navigating tracing efforts.

---

3 Foreign jurisdictions will generally refuse to grant MLA to investigations or prosecutions led by non-judicial agencies or agencies not authorized at law.
4 For a discussion of property-based and value-based confiscation systems, see Module 5
The overall plan or approach often depends on whether the preliminary evidence points to corrupt activities or money laundering. If the former, law enforcement officials investigate the corrupt activities, and then follow the money trail to identify and recover the proceeds of the crime. In the case of money laundering, investigators begin by analyzing financial transactions in order to link them to corruption. Specific steps are likely to include the identification of persons, companies, and assets involved in the case and the connections between them, followed by an analysis of the assets and financial flows.

Particularly in large cases involving significant activity and volumes of documentation, practitioners will find it helpful to set priorities and focus on specific types of documents, accounts or a timeframe. For example, securing, obtaining and analyzing bank account documentation that can be interpreted and mapped out easily is most useful in money laundering cases where investigators need to show links between individuals and companies and reveal the money flow.

Creating a Subject Profile

It is an essential element of all investigations for investigators to collect and record all basic information related to the targets of the investigation. Investigators should collect and record information that fully identifies the targets and also records any aliases used by the targets. All of the information should be maintained in an orderly fashion within the investigators case folder for easy reference. The box below provides a checklist that the investigator should attempt to complete at the early stages of the investigation.

<table>
<thead>
<tr>
<th>Checklist for Collection of Basic Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Date of and place of birth (include aliases); copies of birth certificates, passports.</td>
</tr>
<tr>
<td>✓ Names and dates of birth of both parents (and new partners if divorced or separated), siblings, spouses of siblings, immediate relatives (uncles, aunts, cousins, grandparents, grandchildren).</td>
</tr>
<tr>
<td>✓ Relevant telephone numbers (business, home, mobile), e-mail address and any other Internet or social network communication contact details. In some jurisdictions, it may be possible to obtain subscriber information from the service provider.</td>
</tr>
<tr>
<td>✓ Recent photograph of all targets and associates (preferably government-issued identification).</td>
</tr>
<tr>
<td>✓ Results of a criminal record search</td>
</tr>
<tr>
<td>✓ Results of public source searches on targets and associates. Use Internet search engines, social networking sites, local media reports, and libraries.</td>
</tr>
<tr>
<td>✓ Information from other government agencies, in particular</td>
</tr>
<tr>
<td>✓ Land, vehicle, utility information</td>
</tr>
<tr>
<td>✓ Business records</td>
</tr>
</tbody>
</table>
Avenues for Obtaining Financial Data and Other Evidence

As the targets are identified, practitioners will need to obtain information and financial data and ensure that reliable and admissible evidence is secured for trial. Depending on the investigation plan, the financial data may include all assets and liabilities, income and expenses of the targets and their businesses. Documents and other leads will need to be gathered from a range of sources, including the Internet and other publicly available sources; government agencies; financial institutions including e-banking; money service providers; law and accounting firms; trust and company service providers; real estate agents; art dealers; business competitors; travel and other reward programs; businesses, relatives, employees and associates of the targets; and the targets themselves.

Various investigative techniques, described below, are used to assist practitioners in these efforts. The techniques provided are examples of those used around the world, however not all techniques are available or permitted in every jurisdiction. In addition, jurisdictions will have differences in which techniques require judicial authorization or the application of a special procedure (typically for coercive measures such as search warrants, bank account information, electronic surveillance) and which do not (typically non-coercive measures such as obtaining publically available information and intelligence from other government agencies).

It is imperative that practitioners determine which techniques are authorized in law and that all legal requirements, policies and procedures are followed. Respect for rule of law and the due process rights of the accused will also be essential, particularly if international assistance is being sought. Deviating from legal requirements, policies and procedures or infringements on the rights of the accused can be catastrophic to a case: it can lead to the invalidation and inadmissibility of evidence discovered through the use of that technique and possibly the entire investigation.

---

5 This section is not meant to be an exhaustive ‘how-to’ manual for each technique. More detailed “how-to” guides may be available through public sources (e.g., on-line, libraries, bookstores). In addition, many agencies—both domestic and foreign—have customized guides which they are often willing to share.

6 Many jurisdictions will refuse to provide mutual legal assistance if they perceive that the rights of the accused have not been respected. For information on these basic rights, see the United Nations International Covenant on Civil and Political Rights and the Universal Declaration of Human Rights.
With regard to the selection of a particular technique, this should be assessed as part of the overall investigative plan or framework. Typically, the investigator should first use the most basic investigative techniques (simple data checks) before implementing more complex techniques (wiretaps). In addition, investigators should use covert techniques (e.g., surveillance, public information search, information from other government agencies, trash run) before moving to overt techniques (e.g., search warrant) to avoid tipping-off the target. Practitioners must also keep in mind that the use of one technique can provide leads or information that will become grounds to take additional measures. A search of the trash or a business or residence may reveal documents that link the targets to bank accounts and these facts can be used to support a subsequent order to obtain bank account documentation because they demonstrate a nexus between the targets and the bank accounts. Physical surveillance may reveal a potential gatekeeper to be investigated, and documents obtained further to a production order on a bank may reveal the names of bank officials or individuals involved in a transaction that may be able to provide additional leads if interviewed. For an example of how investigative techniques can be used in practice, see box below.

### Tracing and Recovering Assets -- Efforts in the United Kingdom

Investigators in the United Kingdom became aware of allegations of corruption and misappropriation of assets by former Plateau State Governor in Nigeria Joshua Dariye and suspected assets could be located in the United Kingdom. Through various investigative techniques, they were eventually able to trace the assets and determine the link with the assets and the offense.

1. **Investigative Technique:** Public record searches for information on Dariye in United Kingdom (e.g., property, vehicle, and corporate registries). Sought intelligence from other governmental agencies on Dariye, including financial intelligence unit.
   - **Result:** No link to Dariye found.

2. **Investigative Technique:** Identified family and associates of Dariye and checked for nexus to the United Kingdom.
   - **Result:** Discovered the children of Dariye were attending private school in the United Kingdom.

3. **Investigative Technique:** Inquiries to bank (permitted authority of financial investigators)
   - **Result:** Discovered that Dariye operated a Barclaycard account and that the account was being paid off each month through the bank account of Joyce Oyebanjo.
   - **Result:** Investigations reveal that Oyebanjo was effectively Dariye’s banker in the UK. She paid other fees and utilities on behalf of Dariye, including fees paid to a private school for his two children.

4. **Investigative Technique:** Production order to obtain access to the school files.
   - **Result:** Investigators confirmed that school fees were paid by Joyce Oyebanjo.

5. **Investigative Technique:** Search of publically available information, other governmental agencies for information on Oyebanjo. Also production order on bank accounts of Oyebanjo.
   - **Result:** Oyebanjo, employed as a housing officer in the United Kingdom, is found to have 15 bank accounts with funds totaling roughly £1.5 million, and £2 million worth of...
real property. Further, Oyebanjo is managing one of Dariye’s properties in Regents Park Plaza, a property purchased in the name of “Joseph Dagwan” and paid for by the Plateau State Ecological Fund through various companies.

6. **Investigative Technique:** Credit reference checks revealed bank accounts operated by the suspects. Assets were then traced from the bank account to other bank accounts, property, and vehicles. Production and search orders were used to obtain additional information and trace assets.
   - **Result:** It was discovered that Dariye had one bank account registered to a particular address in London. Examination of Dariye’s and Oyebanjo’s bank accounts revealed large electronic credits from various banks in Nigeria.

7. **Investigative Technique:** Production order to obtain the conveyancing solicitors file for the London address.
   - **Result:** File revealed that property had been purchased using a false name and paid for from a Nigerian company’s London-based bank account.

8. **Investigative Technique:** Mutual legal assistance letter of request was sent to Nigeria to determine the origins of the funds received.
   - **Result:** It was established that an Ecological Grant obtained by Dariye had been diverted and concealed into his own company bank account with the assistance of bank staff. The funds were diverted to a company and associated bank account in Nigeria (set up by Dariye) and subsequently transferred to London for his use. The Nigerian company that purchased the London Property was also linked to the Ecological Grand theft as they received £100 million of the stolen funds. The company had paid £400,000 for the London property after Dariye had authorized a Plateau Government contract for the installation of £37 million worth of television equipment in the Plateau State.

This example illustrates that it is imperative for practitioners to “know their subjects” and to identify all close relatives, business associates, and other persons that could possibly assist a suspect in stealing funds and moving them into foreign jurisdictions. Practitioners must use all techniques available (e.g., other government agencies, public sources, coercive measures) and will never know the origins of the next lead.

### Information from Public Sources and Other Government Agencies

Investigators should gather information on the assets held by targets, their families and associates, and associated businesses from public sources and other government agencies. Public information can be accessed on the Internet using search engines and social networking sites (including archived information), as well as from commercial databases, media sources, libraries and some government agencies. Practitioners may consider subscribing to commercial database providers that hold relevant information.

Information from other government agencies should also be explored (see Figure 1 below):
Figure 1: Preliminary Information Available from Other Government Agencies

- **Financial Intelligence Unit (FIU).** As described in detail in module 2, the FIU is a good source of financial intelligence as FIUs collect STRs and CTRs from financial institutions and designated non-financial businesses and professions and the FIUs will conduct an analysis of all STRs that are submitted, a process which can include a thorough analysis of the individuals and/or business linked to the STR. Intelligence is also shared among FIUs through the Egmont Group. These are all sources of data that can yield intelligence that will help in reconstructing the money trail. Practitioners submitting a request to the FIU should include the following:

  a. Any STR or CTR filed related to targets of the investigation;
  b. Any STR or CTR filed related to businesses linked to the targets;

---

7 In some jurisdictions, the FIU is not permitted to provide a copy of the STR or CTR to law enforcement. In these circumstances, the intelligence report (if drafted) is usually available to be requested and contains much of the same information.
c. Any STR or CTR filed related to any associates/relatives of the targets;  
d. Any related intelligence reports of possible criminal conduct (some FIUs are not permitted to provide information in the absence of an STR).

- **Immigration and Border Crossing Information.** Obtain copies of any governmental forms or any other relevant documents that indicate the border crossings of the targets of the investigation.

- **Customs.** Obtain copies any customs declarations forms that indicate the cross border movement of the targets of the investigation and if there is a cash declaration requirement, check to see if the targets have declared currency.

- **Tax Authorities.** Obtain copies of all tax records related to the targets of the investigation to include individual income tax, property tax, and business tax. The tax assessors’ office or cadastral office can often provide ownership information, a legal description of the property, property value, and purchase history of the property.

- **Auditing Agencies (Office of the Inspector General).** Government auditing agencies (referred to in some jurisdictions as the Office of the Inspector General) is typically mandated with providing an independent and objective review of the operations of the government departments to which they are assigned. They conduct investigations, audits and special projects, detect fraud and misconduct, and promote integrity, efficiency, economy and effectiveness in the department operations. If the corruption has involved a government department, these agencies may have information or resources to assist the investigation.

- **Ethics or Integrity Office (or similar type of office):** The office that is responsible for collecting and analyzing asset and income declarations may be able to provide copies of declarations filed by the targets and close relatives.

- **Land and Vehicle Registries:** Depending on the jurisdiction, the city, county or provincial records office might be able to provide vehicle title information, deeds of property (buyer and seller) and any liens on the property and possible mortgage information.

- **Corporate or Business Registries and Licensing Boards.** Business registries and regulatory boards can provide information that can help identify assets of targets and their associates and records may also identify possible co-conspirators. Some registries will provide the investigator with ownership information, agent of record (typically a
lawyer or accountant), shareholders, board of directors, beneficial owners, and, company financial statements. This search should be conducted for all types of businesses, whether sole proprietorship, partnership, limited liability partnership, or corporation.

- **Civil Records.** Civil registries can provide information about current and previous spouses, siblings, parents, grandparents, and other relatives.

- **Court Records.** Conduct records checks to determine if any of the targets have been involved in prior court matters. If so, review any plea agreements and the transcripts of any testimony, decision, or sentencing hearing for information on assets or other relevant information. Also, check courts that may not be linked to law enforcement databases, including bankruptcy, civil, or family courts.

- **Utilities.** Conduct inquiries into the utility bill of all residence and businesses identified, including electric, water, telephone, cable or satellite, sewage, and garbage. Determine the recipient of the utility bill, method of payment, who executes the payments and subscriber information, if possible. Also, request a general search of targets and associates to determine links to other addresses.

**Other venues to Obtaining Financial Data and Other Evidence**

- **Physical Surveillance.** Physical surveillance is the covert observation of targets of the investigation in order to gather information about them. Recording the movements of targets of an investigation can help investigators identify: possible witnesses; co-conspirators; real property or other assets; lawyers, bankers or accountants possibly involved in facilitating the laundering of corrupt proceeds; businesses; patterns of conduct; and other forms of intelligence that could be vital to the investigation.

- **Trash Runs.** Conducting trash runs involves looking through a target’s garbage for relevant information such as discarded bank statements, names of business associates, etc. In turn, this evidence can be used to support applications for search warrants by showing a nexus between a target and others individuals or assets.

- **Mail Cover.** Mail cover is the process by which a record is made of any data appearing on the outside cover of sealed or unsealed mail (for example, return address, date and location of postage stamp) or of the contents of any unsealed mail. Mail covers can be excellent in providing leads to the location of assets. Mail received from a bank, law firm, company, or accounting firm, for example, alerts investigators to potential sources for information on the assets owned by the target.
• **Account Monitoring Orders.** An account monitoring order is an ex parte order by the court (or the investigative judge in some jurisdictions) which orders that the financial institution specified must, for the period stated in the order, provide account information of the account specified in the order to an appropriate officer in the manner, and at or by specified times stated in the order.\(^8\) The order is beneficial in asset tracing because it allows for real-time financial surveillance of the ongoing transactions in an account which investigators can use to establish typologies of activity and identify new accounts. It can also be a means to gather sufficient grounds for obtaining a disclosure, freezing, or search and seizure order.\(^9\) In cases of large cash withdrawals, it may also present opportunities for cash seizure as the locations will be revealed.

• **Search and Seizure Warrant.** The execution of a search warrant on houses and businesses is a tremendous opportunity to gather evidence of criminal activity, discover information about assets, identify co-conspirators, and develop other leads that support the investigation.\(^10\)

• **Orders for Disclosure or Production of Documents.** Obtaining business documents can be essential to a money laundering/corruption case. Documents that are likely to require judicial authorization will include those held by banks, accounting and law firms, and insurance companies, web-based email services, and sometimes utility companies.

<table>
<thead>
<tr>
<th>Documentation to be requested from financial institutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests to banks will need to be worded as broadly as possible to ensure that all information is obtained. The request will need to seek all records in possession, power or control of [name of bank, branch] relating to [account name and number] and any other account or service related to the account or [name of targets, related persons, close associates, related companies], including, but not limited to the following:</td>
</tr>
<tr>
<td>1. All account opening documentation, including forms which identify the beneficial owner (e.g., “Form A” is used in Switzerland), power of attorney, signature cards;</td>
</tr>
<tr>
<td>2. Client profile, KYC notes, account manager notes, teller or banker journal, cashier check log, and any enhanced due diligence conducted by the financial institution, and any other data probing economic background of client, commercial activities and transactions on the account (e.g., copies of contracts, bills, letter of credits, list of partners and affiliated companies);</td>
</tr>
<tr>
<td>3. Loan documentation, to include mortgage information, copy of loan application, listing and/or description of any collateral, income, assets, and personal and/or business references;</td>
</tr>
<tr>
<td>4. All bank account statements for the period under investigation;</td>
</tr>
<tr>
<td>5. Any reports of suspicious activity that were submitted by an employee of the financial institution, to include those that might not have been forwarded to the FIU;</td>
</tr>
</tbody>
</table>

\(^8\) In the United Kingdom, the order can be in place for up to 90 days at a time.

\(^9\) Typically the standard or proof or other requirements for account monitoring orders are less stringent than for disclosure, freezing, or seizure orders.

\(^10\) In some cases or jurisdictions, this will also be the primary technique used to obtain bank documents.
6. Details of all credits and debits to the account(s) to include electronic funds transfer data, displaying origin, destination, account name and number;
7. Wire transfer documentation, including the request form (see also 3.4.4 and box xx for relevant information related to wire transfers);
8. Correspondence files maintained by the financial institution that could include internal bank memos, records of client visits, phone order notes, e-mails, faxes, notes authored by account managers, records or notes related to instructions or transactions or both;
9. Credit card information to include statements, application, payment history, transaction logs to include any interaction with credit card staff, other cards under the umbrella of the target’s account but in another person’s name;
10. Safety deposit information, including contracts, visiting records, and video surveillance of relevant areas (not viewing areas).

- **Electronic Surveillance.** The surreptitious interception of any wire, oral, telephone, computer, or other electronic communication used by the targets—referred to as “electronic surveillance” in this Handbook—can be very useful to law enforcement in providing investigatory leads similar to those discussed under physical surveillance.

- **Undercover Operations.** Undercover operations are another investigative technique that can be used to infiltrate targets in order to uncover evidence and information about assets. In asset recovery cases, this might include the controlled delivery of funds through an undercover agent. However, such operations are complicated legally and procedurally, risky, and resource-intensive.

**Interviewing targets and non-targets**

Interviews are an essential element of any investigation and tremendously important in money laundering/corruption cases. Statements can corroborate or clarify the information derived from documentary evidence, reveal new leads, or identify new financial documents. Important sources will be any complainants; the business associates, relatives, neighbors, employees, or other associates of the targets; business competitors; financial institution employees and other sources that have been in contact with the targets; as well as the targets themselves.

“Straw men”, individuals that have been duped or paid a rather small service fee for opening an account, will be important to identify and interview. These individuals have taken substantial risk, with little reward, and may prefer to inform authorities of the people they are hiding rather than be implicated in a scheme. Practitioners will need to be familiar with the laws related to

---

11 Some jurisdictions make distinctions between interviews and interrogations, some defining an interview as questioning of non-targets of the investigation while an interrogation is the questioning of targets of the investigation. For the purpose of this section we will use the term “interview” to include both.
conducting interviews with targets and non-targets, especially when working with foreign jurisdictions.12 Some jurisdictions, for example, will have requirements that all statements are taken through a formal hearing. Others will permit a range of interview options, such as routine questioning of witnesses by law enforcement (no formal or verbatim record), written statements, video or audio recorded statements with warning to interviewee, or recorded statements on oath.

Preparing for the interview and having a complete understanding of all the evidence, the targets, associates, timeline of events, and information already gathered in the investigation is essential to conducting a successful interview of both targets and non-targets. A practitioner may prepare questions to cover the information desired; however during the interview, the investigator will need to focus on the responses of the targets, not on the pre-planned questions.13 Since targets may attempt to communicate with one another in order to agree on a common version of events or influence the testimony of a witness, practitioners must take or request from competent judicial authorities appropriate measures to ensure that the targets are prohibited or prevented from communicating with one another or with witnesses prior to the interviews. In addition, a location should be selected that offers the fewest distractions and is most likely to solicit open responses (for example, at a residence, police station, place of business).

**Identifying Relevant Data: Examples from Commonly Sourced Documents**

Various documents will surface throughout an investigation, including bank account records, financial statements, contracts, invoices, deeds, shareholder agreements, articles of incorporation, receipts, etc. They will reveal information on assets, movement of funds, individuals and companies linked to the targets, and other relevant data. To assist practitioners, some examples of relevant data from commonly sourced documents are outlined below.

**Account Opening Documents and KYC/CDD Records**

Practitioners should carefully review all account opening information and any KYC or CDD efforts conducted by the financial institution. In the case of politically exposed persons (PEPs), financial institutions should have additional due diligence on the economic background and transactions in the file. This documentation will likely provide the practitioners with a lot of useful information and potential leads. For example:

- the account manager and persons named as power of attorney may be worth interviewing.

---

12 Practitioners will need to ensure that interview requirements (e.g., required warning to interviewee) are conveyed to foreign counterparts and may have the opportunity to participate. For a discussion on cooperating with foreign practitioners or participating in the execution of the request see chapter 7 and 8.4.6.

13 In this regard, practitioners may find it more helpful to prepare themes rather than specific questions to guide the interview.
• the documents provided by the bank account holder to justify the source of funds. (e.g., contracts, letters, real estate sales) may help to:
  a. identify the beneficial owner (look at addresses, companies and individuals involved);
  b. have a better understanding of the alleged economical background of the funds; and
  c. find contradictions with the figures or with other evidence already gathered;
  d. prepare for interviews with targets.

• in the case of bank accounts in the name of a corporate vehicle, the documents incorporating the company, the name of the board members, and the name of the persons entitled to conduct business on behalf of the company may reveal persons worth interviewing.14

_Bank Account Statements_

As a first step, practitioners should initially focus on determining the origin of the funds entering the account and where the funds have been transferred. This includes debit and credit flows in the accounts through cash deposits and withdrawals, wire transfers, bonds, checks, loans, etc. In reviewing these flows, different techniques will need to be used for assessing the origin and destination of the funds. Below are a few suggestions.

• **Cash:** Cash movements can be an impediment to tracing because of the lack of origin or destination information. Practitioners should obtain the cash deposit or withdrawal receipt from the bank which should indicate the identity of the person initiating the transactions. In addition, practitioners will need to use traditional investigative techniques to follow the link to the cash deposits through e-mails, letters, electronic surveillance, as well as looking at activity in other accounts and safety deposit visiting records.

• **Bonds:** Bonds deposits can be arranged from bank to bank, so practitioners will need to ask the banks for all information regarding the bonds and the method in which they were deposited into the account.

• **Checks:** If it is a check deposit, practitioners may have to go to the bank account from where the check was drawn to identify the originator. If the check is endorsed—signed on the back in order to cash it, deposit it or sign it over to someone else—it should be treated similar to a cash deposit, requiring that the practitioner identify the person who endorsed the check. Practitioners should also review the “memo” line of the check as this

---

14 In some cases, board members and employees of a gatekeeper or service provider responsible for creating shell companies may have little information to assist the investigation.
may indicate suspicious activities. For example, checks to related companies for “management or consulting services” may reveal that the company is laundering proceeds through a series of companies that it owns.

Wire Transfers

Previous corruption cases have shown that large amount of proceeds of crime and corruption are placed into financial institutions and then moved around the world through wire transfers (also referred to as “electronic funds transfers”) in an effort to break the audit trail and place funds in bank secrecy havens.

Financial investigators will need to ensure that wire transfer documentation is requested from financial institutions as this will be critical to asset tracing efforts. This will include a copy of the wire transfer message itself, as well as other documents that financial institutions generate in the process of originating or receiving the transfer of funds.

Accounting Records

In business accounting, all transactions are justified by documentation, recorded through journal or ledger entries that show account names, amounts, and debit or credit information, and summarized in income statements and balance sheets. These records will often be manipulated by corrupt officials and those involved in the schemes in order to disguise their illegal activities. As a result, a detailed review and analysis of accounting records and financial statements uncover anomalies which can help in detecting illegal schemes, for example:

- Invalid invoices may indicate fictitious revenues or purchases;
- Inconsistencies in the work performed by employees may reveal illicit payments disguised as salaries;
- Anomalies in the source of capital and loans provided by shareholders and lenders or absence of evidence that loans were repaid may reveal the misuse of corporate vehicles for money laundering purposes;
- Unusual source and the use of purchased property, the inaccuracy of its valuation, as well as unusual revenue to assets ratios may indicate the misuse of corporate assets; and
- Anomalies in receivables (including unusual high level of credit, litigation or depreciation for specific clients), bank account balances, and transactions in cash may show the misuse of corporate cash flows for illicit purposes.

15 A journal is a record that keeps accounting transactions in chronological order. The most common used are cash receipts, disbursements, sales, purchases, and general journals. A ledger records transactions by type of account. An income statement lists revenue and expenses and a balance sheet lists assets and liabilities.
In cases of bribery or other inappropriate payments from public entities to third parties, government contractors typically invoice a public entity i) for goods and services at an inflated amount as compared to the actual market price, or ii) for goods and services that were never provided.

**Purchase and Sale Documents**

Documents related to the purchase and sale of assets—whether property, shares, vehicles, jewelry, or art—will include land registry documents, purchase and sale agreements, loans, mortgages, financial statements, tax returns, and credit card statements. Practitioners should focus on documenting the value and dates of purchase and sale, name of buyer or seller, method of payment (cash, check, currency), and source of funds. With assets purchased with cash, it may be difficult to trace the date of purchase or value, particularly when there are numerous potential sellers or dealers (e.g., art, jewelry, vehicles). Travel information (gathered from border crossing information, credit card information, or travel reward programs), insurance policies, jewelry repair bills, vehicle information numbers, dealer stickers or decals on the vehicles, and art dealers may provide assistance in determining the seller of these items and dates of purchase.

**Tracing assets (or managing evidence)**

It will be important to organize the information gathered into an account profile for each bank account and this information, in turn, can be combined with other financial data collected (e.g., other asset holdings, liabilities, income, expenses) to build a financial profile for the targets. A standard computer spreadsheet program could be used for this purpose.16

As an example, the account profile should include the following information:

- name of the bank and branch location;
- bank account number and type;
- bank account holder, beneficial owner, power of attorney;
- date of account opening/closing;
- currency;
- account balance as at the time of the disclosure;
- annual credit turnover
- annual debit turnover

---

• whether or not the assets have been restrained

To assist with the organization of data, as well as eventual presentation and explanation, practitioners should map out the flow of funds in a flow chart. These flow charts provide a visual snapshot of the targets, associates, gatekeepers, and corporations involved, as well as the assets, bank accounts, and corporate vehicles. Not only is this snapshot or ‘big picture’ view helpful for practitioners as they attempt to understand and interpret the flows, but it becomes essential when explaining the flow and associations developed during the course of the investigation to a prosecutor or judge.

Figure 2: Sample flow chart

Figure 3: Sample Chart of Relationships and Assets
In addition, practitioners should consider use of a document management system, particularly in complicated cases and large amounts of data.

Comparing the Flows against the Financial Profile is a critical phase, analysts will compare and contrast dates, origins, destinations, bank account holders, banks, and sources of information to group and reconcile transactions and identify gaps in data. For example, one account may show the withdrawal of a large sum of cash—leaving the analyst without destination information—but another may show a subsequent deposit. Or perhaps physical surveillance records reveal that the target travelled to a foreign jurisdiction in the days following the withdrawal. Payments to contractors maybe linked to subsequent deposits: In one case, several deposits by a corrupt official were found to be the same percentage of the payments to the contractor. This analysis will help in better understanding the asset flow and in the development of new leads.

Another technique used by practitioners is a net worth analysis, the process of comparing the value of the assets held by the target with reported income. Any unreported income is likely to have illicit origins and practitioners will subsequently need to direct efforts to show a link between the asset and the offense. In jurisdictions that prosecute illicit enrichment, the net worth analysis is a necessary step in the investigation.
To assist in identifying corruption and money laundering schemes, it can be helpful to review information or research on the various typologies and red flags for identifying criminal activity. Many agencies and international organizations publish such reports and they are available online, including:

- FATF typology reports (e.g., FATF Typologies on Money Laundering and Terrorist Financing in the Real Estate Sector),
- FIU annual reports on STRs,
- Reports by the FIU, financial sector supervisor, or banking association on typologies and red flags for identifying criminal activity and money laundering.
Summary and Review of Module 4

In this module, we learnt that successful investigation of corruption and money laundering requires a comprehensive plan of action that incorporates a number of important steps and considerations. Practitioners will need to gather and assess the facts in order to understand the case, assemble a team, identify key allies, and communicate with foreign counterparts. Moreover, it was observed that especially in large and complex cases, it is essential to assemble a multi-disciplinary team from diverse disciplines and agencies.

A discussion was then had on how and what practitioners will need to obtain information and financial data and ensure that reliable and admissible evidence is secured for trial. It was indicated in the module that depending on the investigation plan, the financial data may include all assets and liabilities, income and expenses of the targets and their businesses.

Furthermore, it was suggested in this module that documents relevant to the investigation will need to be gathered from a range of sources, including the internet and other publicly available sources; government agencies; financial institutions including e-banking; money service providers; law and accounting firms; trust and company service providers; real estate agents; art dealers; business competitors; travel and other reward programs; businesses, relatives, employees and associates of the targets; and the targets themselves.

Various examples were provided on what information needs to be gathered in an investigation; how this information can be gathered; and how to identify what is relevant information to assure a successful trial that is enable to survive the scrutiny of a trial.

The module then concluded by looking at the aspect of tracing assets and the importance of organizing the information gathered into an account profile for each bank account, how this information, in turn, can be combined with other financial data collected (e.g., other asset holdings, liabilities, income, expenses) to build a financial profile for the targets.