Module 2

Role of the Financial Intelligence Unit

(incorporating peer reviewers comments)
Table of Contents

Overview ........................................................................................................................................................... 3
Definition/types of FIUs ........................................................................................................................................ 4
   Introduction ............................................................................................................................................. 4
   Administrative-type FIUs .......................................................................................................................... 5
   Law-enforcement-type FIUs ...................................................................................................................... 7
   Judicial or prosecutorial-type FIUs ........................................................................................................... 8
   “Hybrid” FIUs .............................................................................................................................................. 9
Reception of information-FIU as a national center and relation with reporting entities ................................. 11
   Reporting entities ....................................................................................................................................... 11
   Types of financial information collected by the FIUs ................................................................................ 16
      Suspicious Transaction Reports ........................................................................................................... 16
Example of an STR ............................................................................................................................................ 18
   Cross Border Currency Transportation Reports ..................................................................................... 19
      Threshold Reports ................................................................................................................................ 20
Analysis of reports .......................................................................................................................................... 20
   Tactical analysis: ........................................................................................................................................ 21
   Operational Analysis ................................................................................................................................. 22
   Strategic analysis ........................................................................................................................................ 22
Dissemination of information- Relation with other agencies ......................................................................... 23
   Information sharing .................................................................................................................................. 27
Developing a Strategy for More Effective Anti-Corruption Agency – FIU Cooperation ................................. 30
Summary and Review of Module 2 ................................................................................................................ 32
Overview

This module will provide explanations on what is a Financial Intelligence Unit (FIU); what are the different types of Financial Intelligence Units; what are the main functions of Financial Intelligence Units; what is a Suspicious Transaction or Suspicious Activity Report (STR/SAR); what is a cross border currency transaction report or a customs monetary instrument report (CMIR); what are Currency Transaction Reports (CTR); what are tactical, operational and strategic analysis that is typically conducted by Financial Intelligence Units; in what ways Financial Intelligence Units can provide assistance in corruption cases; and some cases that demonstrate how Financial Intelligence Units can support law enforcement investigations.

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

- Know what a Financial Intelligence Unit is and what are its functions;
- Know what are the different types of Financial Intelligence Units;
- Know the advantages and disadvantages of each type of Financial Intelligence Unit;
- Know, how and in what ways a Financial Intelligence Unit can assist anti-corruption agencies in their investigation of corruption cases;
- Describe the nature and function of their respective Financial Intelligence Unit.
Definition/types of FIUs

Introduction

At the beginning of the modern anti-money-laundering strategy in the mid 1980s countries developing their anti-money-laundering strategies found that law-enforcement agencies had limited access to relevant financial information. It became clear that a new strategy required them to “engage the financial system in the effort to combat laundering while, at the same time, seeking to ensure the retention of the conditions necessary for its efficient operation.”¹ Countries also found that implementation of a system requiring disclosures of suspicious transactions or suspicious activities on the part of financial institutions created the need for a central office or agency for assessing and processing these disclosures². The first financial intelligence units (FIUs) were established in the early 1990s in response to the need for a central agency to receive, analyze, and disseminate financial information to combat money laundering. Over the following ten years, the number of FIUs increased to the point where the Egmont Group, an international association of FIUs, has 116 members by 2010. Moreover, not all FIUs are members of Egmont, but international standards require at a minimum that where a country has created an FIU, it should consider applying for membership to the Egmont Group. Therefore, once FIUs become operational, they typically apply for Egmont membership. Even though members and non-members of the Egmont Group share the same core functions of receiving, analyzing, and disseminating financial information to combat money laundering and financing of terrorism, they differ in many ways.

**Definition of an FIU**

A central national agency responsible for **receiving** (and as permitted, requesting), **analyzing** and **disseminating** to the competent authorities, disclosures of financial information: i) concerning suspected proceeds of crime, or ii) required by national legislation or regulation, in order to combat money laundering.

Similar to an Anti Corruption Agencies (ACA’s) an essential element of an FIU is operational independence and autonomy to ensure that it is free from undue influence or interference. This includes factors affecting the manner in which the FIU may discharge its responsibilities, the degree to which other bodies or actors can instruct or influence the work of the FIU, or can have access to the data holdings of the FIU, or be privy to the findings of the FIU on individual cases.

Over the years, countries have established FIUs for the general purpose of combating money laundering and terrorism financing have generally given them the three core functions that are part of the accepted definition of an FIU. The information needed to support money laundering

---

investigations is often broader than those involving other predicate offenses like narcotics trafficking, weapons smuggling and others. Countering money laundering and other financial crimes effectively requires not only knowledge of laws and regulations, investigations, analysis, and intelligence but also of banking, finance, accounting and other related economic and business related activities. It is exactly the need to combine the more standard criminal investigative skills with the specialized financial investigative skills that require the creation of such entities as FIUs or similar type of body.

**THE THREE BASIC FUNCTIONS OF AN FIU**

The administrative arrangements by which these functions are carried out, however, vary considerably from country to country. These variations arise from different country circumstances, together with the lack of an internationally accepted model for the functions of an FIU in the early 1990s, when the first such units were established. For example, in some countries, the function of the FIU as an additional tool for law-enforcement organizations in combating money laundering and associated crimes was emphasized, and this led to the establishment of the FIU in an investigative or prosecutorial agency. Other countries emphasized the need for a “buffer” between the financial institutions and the police, and consequently their FIUs were established outside these agencies. In practice the FIUs can consist of four different types:

- Administrative-type
- Law-enforcement-type
- Judicial or prosecutorial-type
- “Hybrid”

**Administrative-type FIUs**

Administrative-type FIUs are usually part of the structure, or under the supervision of, an administration or an agency other than law-enforcement or judicial authorities. They sometimes constitute a separate agency, placed under the substantive supervision of a ministry or administration, “autonomous FIUs,” or are not placed under such supervision considered “independent FIUs.”
The main rationale for such an arrangement is to establish a “filter” or “buffer” between the financial sector and other reporting entities such as casinos, NGOs, businesses, other entities and professionals that are subject to reporting obligations and law-enforcement authorities. Often, financial institutions facing a problematic transaction, activity or relationship do not have hard evidence, are not trained investigators and do not have the capacity to determine with certainty that a transaction or activity is connected to a criminal offense. As a result, they will be reluctant to disclose the activity directly to a law-enforcement agency, out of a concern that their suspicion may be unfounded; therefore jeopardizing their relationship with their customers.

One role of the FIU is to conduct analysis to substantiate the suspicion and send the case to the competent authorities in charge of criminal investigations and prosecutions or if the suspicions are unsubstantiated, file the information and not forward the case. In most cases, the decision to establish the FIU outside the law-enforcement system also leads to the decision that the FIU’s powers will be limited to the receipt, analysis, and dissemination of suspicious transaction and other reports, and that they will not be given investigative or prosecutorial powers. Countries that are recovering from a post conflict environment or have a police force with a history of corruption or violence are contributing factors when policy makers decide to create an administrative style FIU. Similarly, the powers of the FIU to disclose the information contained in transaction reports is usually narrowly defined, to preserve the confidential character of the information provided. After all, it is financial intelligence and not evidence!

By making an administrative authority a “filter” or “buffer” between the financial institutions, other reporting entities and law-enforcement sectors, authorities can more easily enlist the cooperation of reporting institutions, which are often conscious of the drawbacks vis-à-vis their clients of having direct institutionalized links with law-enforcement agencies. Administrative-type FIUs are often preferred by the banking sector. They may also appeal to other institutions and professionals that have been added to the list of reporting entities for the same reasons. Among the countries that have established “administrative” FIUs are Nigeria, USA, Egypt and Guatemala.

Some administrative and even hybrid type FIUs have supervisory authority over reporting entities concerning anti-money laundering and terrorist financing matters. This is typically referred to as compliance functions and usually requires the FIUs to dedicate specially trained staff to conduct compliance inspections of reporting entities to ensure that they are in compliance with their countries AML/CFT requirements to include their reporting requirements to the FIU of STR/SAR information. Typically, law enforcement and judicial/prosecutorial type FIUs do not have supervisory or compliance functions.
Advantages:

- Operates as a filter/buffer between reporting entities and law enforcement;
- Financial institutions are more comfortable disclosing information because of limited dissemination after analysis;
- FIU is neutral and technical when conducting analysis;
- Information exchanged easily with all types of FIUs

Disadvantages:

Possible delays in applying law enforcement actions;
Limited range of legal powers.

Law-enforcement-type FIUs

In some countries, the emphasis on the law-enforcement aspects of the FIU led to the creation of the FIU as part of a law-enforcement agency, since this was the easiest way to establish a body with appropriate law-enforcement powers without having to design from scratch a new entity and a new legal and administrative framework. It will nevertheless require some authorizing rule formally creating such an entity. Operationally, under this arrangement, the FIU will be close to other law-enforcement units, such as a financial crimes unit, and will benefit from their expertise and sources of information. In return, information received by the FIU can be accessed more easily by law-enforcement agencies and can be used in any investigation, thus increasing its usefulness. Exchange of information may also be expedited through the use of existing national and international criminal information exchange networks. Also, a law-enforcement-type FIU will normally have the law enforcement powers of the law-enforcement agency itself (without specific legislative authority being required), including the power to freeze transactions and seize assets (with the same degree of judicial supervision as applies to other law-enforcement powers in the country). This is likely to facilitate the timely exercise of law-enforcement powers when this is needed. Moreover, staffing for this type of FIU is typically drawn from existing law enforcement personnel with financial and/or intelligence backgrounds. Among the countries that have established “Law-enforcement” FIUs are UK, Papua New Guinea and Estonia.

Advantages:

- Built on existing infrastructure;
- Maximize law enforcement usage of information received;
- Quicker law enforcement reaction to information;
- Law enforcement to law enforcement exchange of information;
- Information easily combined with criminal intelligence.
**Disadvantages:**

- Focused on investigations rather than preventive measures;
- Unusual relationship with financial institutions and other reporting entities;
- Typically does not receive CTRs or CMIRs;
- Conduct operations in a law enforcement exclusion manner rather than inclusion.

**Judicial or prosecutorial-type FIUs**

This type of FIU is established within the judicial branch of the state and most frequently under the prosecutor’s jurisdiction. Instances of such an arrangement are found in countries with a continental law tradition, where the public prosecutors are part of the judicial system and have authority over the investigatory bodies, allowing the former to direct and supervise criminal investigations. Disclosures of suspicious financial activity are usually received by the prosecutor’s office, which may open an investigation if suspicion is confirmed by the first inquiries carried out under its supervision. The judiciary’s powers (e.g., seizing funds, freezing accounts, conducting interrogations, detaining suspects, and conducting searches) can then be brought into play without delay. Judicial and prosecutorial FIUs can work well in countries where banking secrecy laws are so strong that a direct link with the judicial or prosecutorial authorities is needed to ensure the cooperation of financial institutions. It may be noted that the choice of the prosecutor’s office as the location of an FIU does not exclude the possibility of establishing a police service with special responsibility for financial investigations. Also, in many countries, the independence of the judiciary inspires confidence in financial circles. Among the countries that have established “Judicial or Prosecutorial” FIUs are Denmark, Cyprus and Vanuatu.

**Advantages:**

- High degree of independence from political interference;
- Disclosure information is received directly by the institution mandated to investigate and prosecute;
- Judicial powers brought into play.

**Disadvantages:**

- Possible difficulties in exchanging information with non-judicial or prosecutorial FIUs;
- Focused on investigations rather than preventive measures;
- Typically does not receive CTRs or CMIRs.
“Hybrid” FIUs

This last category encompasses FIUs that contain different combinations of the arrangements described previously. This hybrid type of arrangement is an attempt to obtain the advantages of all the elements put together. Some FIUs combine the features of administrative-type and law-enforcement-type FIUs, while others combine the powers of the customs office with those of the police. For some countries, this is the result of joining two agencies that had been involved in combating money laundering into one. It may be noted that in some FIUs listed as administrative-type, staff from various regulatory and law enforcement agencies work in the FIU while continuing to exercise the powers of their agency of origin. Among the countries that have established “hybrid” FIUs are Australia, Andorra, St. Vincent & Grenadines and Philippines. This “Hybrid” type of FIU is relatively rare and often is administrative in nature but is staffed from various regulatory and law enforcement agencies that work at or are seconded to the FIU and these personnel often maintain and exercise the powers of their original agency.

Although the types of FIUs vary in many ways, most share a common definition, which refers to their basic function: serving as a national center for the collection, analysis, and dissemination of information regarding money laundering and the financing of terrorism. These three functions are the core functions of almost all FIUs.

Exercise:
What type of FIU do you have? If you have this type of FIU in your jurisdiction, would you agree with the assessment on the advantages and disadvantages of such an FIU? Based on your jurisdiction’s experience, are there any other advantages or disadvantages you can identify?

Example of an FIU: The Dutch Office for the Disclosure of Unusual Transactions (MOT)

The MOT is an administrative unit within the Dutch Ministry of Justice. It is divided into five substantive departments that deal with the processing of suspicious transaction reports, system management, policy and law enforcement liaison, analysis and international cooperation. MOT has around 20 employees. The eight members of the processing unit have a financial or law enforcement background while the others come from varied professional backgrounds.

MOT serves as a filter/buffer unit. In other words, financial institutions report to MOT when they encounter transactions that are unusual either objectively (the amount exceeds Euros 40,000) or subjectively (a day laborer receives a €500,000 wire transfer into his account). The unit analyses the information, compiles a report, and then passes on the information to the law enforcement side if there is a suspicion of money-laundering. In order to process the information, MOT has access to different public and police databases that are automatically updated on a daily basis. Moreover, MOT is entitled to ask financial institutions for further information regarding the transaction, although it has no law enforcement competence.
**Other possible functions of an FIU may include:**

Receives cross border transfer reports  
Investigate allegations of money laundering and terrorism financing  
Instigate money-laundering prosecutions  
Investigate suspicious transaction reports  
Advise on matters of money laundering policy  
Instigate asset confiscation proceedings  
Forward every suspicious transaction report to law enforcement  
Report ‘tipping off’ offences for possible prosecution  
Sanction and/or report for possible prosecution reporting institutions for failing to report suspicious transactions  
Provide a database of information for use by law enforcement officers  
Advise on what makes a particular transaction suspicious  
Provide intelligence for obligated institutions  
Coordinate international legal assistance in money laundering cases and terrorism financing  
Evaluate and analyse suspicious transaction reports  
Receive suspicious transaction reports from members of the public  
Provide intelligence to other countries’ financial intelligence units  
Monitor compliance by reporting entities with their obligations under national AML/CFT legislation  
Provide intelligence to Law Enforcement  
Respond to requests for intelligence from Law Enforcement agencies  
Provide advice on amendments to money laundering and terrorism financing legislation  
Give guidance to reporting entities regarding their obligations under national anti-money laundering legislation  
Give guidance to supervisory bodies regarding their obligations under national anti-money laundering legislation

**Exercise:**

1. What of the aforementioned functions and responsibilities does your FIU perform?  
2. In your opinion, what are the most important functions and responsibilities in your jurisdiction and why?  
3. Are there any functions and responsibilities you wish your FIU had, and why?
FIU as a national center and relation with reporting entities

In order to understand how FIUs can support Anti-Corruption Agencies it is necessary to understand the information that is the foundation of its work; where does the information derive from; and, what kind of information do they receive, and what type of analysis do they conduct. In general, the primary task of the FIU is to collect the information from the reporting entities and other sources regarding suspicious or unusual transactions or activities; incorporate them into and compare them to their existing records; analyze all the data, either systematically or by targeting specific data, in order to detect possible illicit transactions and trace the laundered proceeds.

Reporting entities

The Reporting entities can typically be split up in two groups consisting of financial institutions and designated non-financial businesses and professions. Regulated financial institutions, banks in particular have been at the center of the system of reporting suspicious transactions. The sheer volume of transactions undertaken through them, compared with other institutions through which money can be transmitted, makes them the prime target for financial misuse. However reports from nonfinancial institutions are increasingly important as financial institutions are setting up more sophisticated systems to detect and report suspicious transactions, criminals may be tempted to use other institutions and professionals for laundering purposes.

A very important tool for financial institutions and other regulated institutions in identifying suspicious transactions or suspicious activities is the customer due diligence (CDD) or know your customer (KYC) principles. This allows reporting entities a better opportunity to manage and observe their clients by identifying, verifying, and recording the identity of customers, as well as additional information about customers’ background, business, and likely level of and type of activity at the institution.

Accordingly, as part of an efficient anti-money laundering regime, financial and non-financial actors need to:

- Identify and verify the identity of clients and beneficial owners;
- Obtain information on the nature and purpose of client’s business relationships;
- Conduct ongoing due diligence on the client’s business relationships and scrutinize transactions undertaken throughout the course of their relationship with the client in order to ensure that the transactions being conducted are consistent with their

---

3 However, in some settings -- such as when there is ongoing conflict or in post-conflict situations, even minimum CDD/KYC has not happened, e.g. Liberia and Sierra Leone. Thus, as the Taylor case in the Special Court of Sierra Leone shows, PEPs associated with Taylor could then reinvest proceeds easily after the conflict, even while the main PEP is on trial.

4 Beneficial owner is a legal term where specific property rights (“use and title”) in equity belong to a person even though legal title of the property belongs to another person.
knowledge of the client, their business and risk profile, including, where necessary, the source of funds;

- pay special attention to all complex, unusual large transactions, and all unusual patterns of transactions, undertaken by clients that have no apparent economic or visible lawful purpose;

- maintain, for at least five years, all necessary records on transactions relating to, both domestic or international, so as to be able to comply swiftly with information requests from law enforcement authorities and FIUs;

- keep records on the identification data obtained through the customer due diligence process (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence for at least five years after the business relationship is ended.

The information gathered through such diligence and record keeping measures will allow financial and non-financial actors to establish client’s profiles and to compare the collected information to what is actually occurring in accounts. These measures, cumulated with the obligation to report to the FIU any suspicious transaction, constitute a critical source of information that, when needed, will permit the reconstruction of individual transactions. Once adequately analyzed, they will provide evidence for prosecution of criminal activity, especially in corruption cases.
“Reading” a bank statement and knowing a customer

Take a hypothetical case of Mr. Smith. Mr. Smith opened a cheque account with Big Bank Group on 1 January 2010. He provided adequate documentation verifying his identity and address. Big Bank Group has compiled the following information about Mr. Smith’s business:

- **Purpose of account**: Cheque account; day to day transactions
- **Annual income**: US$50,000
- **Source of income**: Employed by Microsoft Corporation
- **Source of wealth**: Monthly salary payments
- **Estimated account activity**: US$4000 per month
- **Type of services used**: Checks; ATM; domestic payments
- **International connections**: Limited. Some international payments made for internet purchases

<table>
<thead>
<tr>
<th>Mr Smith</th>
<th>BIG BANK GROUP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1045 56TH STREET</td>
<td>4587 10TH AVENUE</td>
</tr>
<tr>
<td>SEATTLE</td>
<td>NEW YORK</td>
</tr>
<tr>
<td>WA 38472</td>
<td>USA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2010</th>
<th>Account No</th>
<th>Debit</th>
<th>Credit</th>
<th>Balance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 01</td>
<td>OPENING CREDIT</td>
<td>$2,000.00</td>
<td>$2,000.00</td>
<td></td>
</tr>
<tr>
<td>Sep 10</td>
<td>ELEC TRSF PACIFIC HEIGHTS EXPORTS</td>
<td>$87,345.00</td>
<td>$89,345.00</td>
<td></td>
</tr>
<tr>
<td>Sep 11</td>
<td>CASH</td>
<td>$3,500.00</td>
<td>$92,845.00</td>
<td></td>
</tr>
<tr>
<td>Sep 14</td>
<td>CASH</td>
<td>$2,500.00</td>
<td>$95,345.00</td>
<td></td>
</tr>
<tr>
<td>Sep 20</td>
<td>TIMBER MERCHANTS OF PERU</td>
<td>$80,000.00</td>
<td>$15,345.00</td>
<td></td>
</tr>
<tr>
<td>Sep 26</td>
<td>ELEC TRSF N WEST MINING CO, ANGOLA</td>
<td>$35,489.00</td>
<td>$50,834.00</td>
<td></td>
</tr>
<tr>
<td>Sep 27</td>
<td>FX 25,000 TL @ US$1.5</td>
<td>$16,667.00</td>
<td>$67,501.00</td>
<td></td>
</tr>
<tr>
<td>Sep 27</td>
<td>FX CHARGE</td>
<td>$40.00</td>
<td>$67,461.00</td>
<td></td>
</tr>
<tr>
<td>Sep 30</td>
<td>Charles Taylor</td>
<td>$52,000.00</td>
<td>$15,461.00</td>
<td></td>
</tr>
</tbody>
</table>

Red Flag description generated by Big Bank Group

<table>
<thead>
<tr>
<th>Reason for Flag</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dormant account reactivated</td>
<td>Account last used on 1/1/02</td>
</tr>
<tr>
<td>Unusual turnover</td>
<td>Expected turnover $4000 per month Vs actual of $135,000</td>
</tr>
<tr>
<td>Unusual cash transactions</td>
<td>Cash payments of $6000 credited to account, including foreign currency exchange</td>
</tr>
<tr>
<td>International counterparties</td>
<td>Counterparties unknown; questionable locations e.g. Angola and Peru</td>
</tr>
<tr>
<td>Unusual services</td>
<td>Frequent use of international electronic transfers</td>
</tr>
</tbody>
</table>

After reviewing the red flags the Bank staff considers whether or not a transaction is suspicious.
Though the volume of transactions via the banking sector generally are higher compared to other institutions through which money can be transmitted, the non-banking financial sectors along with designated non-financial businesses and professions can also appear attractive for criminal proceeds to be laundered, perhaps more so in jurisdictions where banking inclusion is limited among the population. Therefore, it is important that the reporting entities that are not limited to only the banking sector, but include all entities that function as a likely entry point of illegal funds.

Categories of reporting entities to FIU

1. “Other” can embody Car Dealers, NGOs, Travel Agencies, Central Bank and other Businesses, etc.
Casinos offer an attractive venue for laundering illegal proceeds, because gambling involves large volumes of cash and many casinos offer their clients a wide variety of financial services buying chips or tokens with cash, or conducting minimal or no betting and then requesting repayment of the balance by a check drawn on the casino’s account or by direct transfer to a bank account.

Together with trust and company service providers, lawyers, notaries, and accountants are seen as gatekeepers, because, owing to the nature of some of their activities, they may be in a position to detect the intended use of legal arrangements, such as trusts and corporate vehicles\(^5\), to launder funds. Indeed, criminals may seek the services of legal professionals to obtain assistance in making illegal transactions appear legal, thus, more difficult to detect. Also, some money launderers like to use the lawyer’s client account as a means of introducing illegal funds into the banking system.

Real estate and other high-value items, such as gold, precious metals and precious stones, offer attractive opportunities for money launderers to invest their illicit proceeds. The purchase of real estate is significant area where launderers invest their illicit proceeds. Precious metals, gold and precious stones can be used in the same manner and also has the added advantage of being easily transportable across borders. Other high value items can include works of art. There is an Art Registry, a private initiative, which mainly looks at forgeries and traffic in stolen art – but the Philippines for example used this registry to trace the ownership of ill-gotten assets.

Exercise:
1. What are the required reporting entities in your jurisdiction?
2. What are the most significant reporting entities in your jurisdiction and why do you believe they are significant?
3. Are there other entities that you think might be relevant and should be required to report?

There are several reasons for institutions to make Suspicious Transaction Reports (STR)/Suspicious Activity Reports (SAR) to the FIUs:

Legal risk - It’s the law! Institutions may become subject to lawsuits resulting from the failure to observe mandatory standards regarding anti money laundering measures. Consequently, institutions can, for example, suffer fines, criminal liabilities and special penalties imposed by supervisors and other competent authorities.

\(^5\) Legal persons, trusts and similar arrangements are collectively referred to as corporate vehicles
Reputational risk - The nature of their business requires maintaining the confidence of depositors, creditors and/or the general marketplace. Being associated/affiliated with money laundering will cause a loss of confidence in the integrity of the institution.

Operational risk - The risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events. A public perception that a bank is not able to manage its operational risk effectively can disrupt or adversely affect the business of the institutions.

Types of financial information collected by the FIUs

Having already discussed the fact that FIUs have a wide range of sources of information, we can start to focus on the types of information an FIU can expect to receive. In general the information consists of following types of information:

- Suspicious Transaction or Suspicious Activity
- Cross Border Currency Transportation Reports
- Threshold Reports or Currency Transaction Reports

Suspicious Transaction Reports

Suspicious Transaction Reports, also referred to as Suspicious Activity Reports, are the most frequent types of reports received by FIUs. This is usually the first stage where the competent authorities become aware of information possibly regarding money laundering. These reports are submitted to the FIU when the institutions described in previous sections have a transaction(s) that they suspect could be linked to a criminal offense.

Given that financial institutions and other regulated institutions generally have a good sense of their customers’ business activity they are reasonably effective in identifying suspicious transactions or activities. Moreover, staff are required to receive training on anti-money laundering and countering terrorist financing measures and typologies of suspicious conduct and how to report such conduct. Sometimes this training is conducted by the FIU or other supervisors to the reporting entities.
1. Example of a suspicious transaction, use of real estate, cars and alternative remittance systems

The subject, Mr X, began business by giving a loan of US$10,000 to five family friends who went abroad and paid back in kind through used vehicles. Mr. X sold the vehicles and bought a parcel of land, established and registered a local Forex Bureau and began money exchange at a starting capital of US$20,000. After six months, he injected US$300,000 into the business and began remitting US$300,000 each quarter in money transfer. He received used vehicles from friends abroad in exchange for providing loans to family members in Liberia, Ghana and Guinea. He justified his wealth by the resale of collaterals obtained from loans issued, foreign exchange, and remittance services. In 2005 he put another huge amount of cash into the business and is now constructing multi-complex stores and residential buildings in the suburb of the capital of country L, which are valued up to US$500,000. The point of suspicion is that Mr. X’s business growth is astronomically unprecedented – from a US$20,000 investment in 2000 to more than half a million in 2005.

2. Example of a suspicious transaction or suspicious activity:

Mr. Hibbard has maintained an account with a bank for the past five years. The bank records show him to be a mid level civil servant on an established income. One day Mr. Hibbard requests that a large wire payment be sent to a third party in another jurisdiction. When looking at the account history, it is seen that the funds in question were credited to his account through a wire payment from another person in the same country as the payment he is now sending. When conducting their CDD checks, the bank asked Mr. Hibbard to further explain the transaction and Mr. Hibbards’ response was vague and unconvincing indicating it was related to a land deal.

Questions:
1. Do you think this fact pattern raises any suspicion?
2. If not, why not?

When an obligor’s employee(s) observes a suspicious transaction they are to file an STR/SAR to the FIU. Below is an example of a typical STR form. However, it is important to note that the form of the STR varies among jurisdictions and also among the different reporting entities but most typically contain information on:

- Customer name and identifiers;
- Place, date and time of transaction/activity;
- Account information;
- Narrative describing the suspicious conduct;
- Reporting entity, supervisor and employee generating STR/SAR
Example of an STR

<table>
<thead>
<tr>
<th>STRICTLY PRIVATE AND CONFIDENTIAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your ref: 0224554</td>
</tr>
</tbody>
</table>

Legislation under which this disclosure is made (please tick one of the following):
Suspicion of money laundering X
Suspicions relating to terrorism □

<table>
<thead>
<tr>
<th>Subject’s full name(s)</th>
<th>Kevin Hibbard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gender</td>
<td>Male</td>
</tr>
<tr>
<td>Date(s) of birth</td>
<td>April 5 1965</td>
</tr>
<tr>
<td>Place(s) of birth</td>
<td>Hospital Lane 8, St Peter Port, England</td>
</tr>
<tr>
<td>Passport or ID number(s)</td>
<td>2544 7358 9700</td>
</tr>
<tr>
<td>Nationality(ies)</td>
<td>English</td>
</tr>
<tr>
<td>Address(es)</td>
<td>Kingston street 47, Birmingham ,England</td>
</tr>
<tr>
<td>Telephone</td>
<td>Home: 248 658 774 Work:</td>
</tr>
<tr>
<td>Occupation/employer</td>
<td>Contracting Officer</td>
</tr>
</tbody>
</table>

Associated company: *e.g. company registration number, date and place of incorporation, etc.*

<table>
<thead>
<tr>
<th>Account name</th>
<th>Kevin Hibbard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account/product number</td>
<td>5587 8474 4457 6884</td>
</tr>
<tr>
<td>Date account/product opened</td>
<td>March 25 2005</td>
</tr>
<tr>
<td>Details of any intermediary</td>
<td>No</td>
</tr>
</tbody>
</table>

Other relevant information: *e.g. additional details of identification and/or references taken, associated parties,*

The transaction implicated transaction to a bank account belonging to Bank of Napoli with the account number 2461 1256 2148
Reasons for suspicion:

Hibbard requested that a large wire payment (£250,000) where sent to a third party in Italy. When looking at the account history, it was revealed that the funds in question were credited to his account through a wire payment from another person in Italy. When the account making the transaction asked Mr. Hibbard to further explain the transaction Mr. Hibbards’ response was vague and unconvincing indicating it was related to a land deal.

Current status of business relationship: Mr. Hibbard is still private customer with a checking account, car and home loan with us.

To help provide information of the customer’s previous transactions there is a general minimum requirement for records to be kept for five years after either completion of the transaction or termination of the account relationship. These requirements also serve to assist the FIU in the further analysis of the case. The records concerned and of interest to the FIU will include:

- Customer identification and additional KYC details;
- Transaction and related details;
- Business correspondence;
- Any other information that would assist in tracing and identifying the beneficiaries of accounts or property.

Questions:

1. What financial institutions, non-financial businesses and professions would you consider a high risk of being misused for money laundering in corruption cases in your jurisdiction?
2. Looking at a completed SAR/STR form from your FIU, what information do you find relevant to you as a corruption investigator/prosecutor?
3. Is there any additional information you believe should be included in the SAR/STR?

Cross Border Currency Transportation Reports

A growing number of international instruments encourage countries to implement a system of reporting cross-border movements of currency. For instance the United Nations Convention against Corruption states: “States Parties shall consider implementing feasible measures to detect and monitor the movement of cash and appropriate negotiable instruments across their borders,
subject to safeguards to ensure proper use of information and without impeding in any way the movement of legitimate capital. Such measures may include a requirement that individuals and businesses report the cross-border transfer of substantial quantities of cash and appropriate negotiable instruments."

Also, the international standards on combating money laundering and terrorism financing, state that countries should have measures in place to detect the physical cross border transportation of currency and bearer negotiable instruments, including a declaration system or other disclosure obligation.

In some countries these reports are known as Customs Monetary Instruments Reports (CMIR – USA). In the Czech Republic, for example, the customs authorities are required to report to the FIU when they ascertain, in the performance of their duties, currency or other negotiable instruments exceeding CZK 350,000 (about US$13,000) entering or exiting the Czech Republic.

Threshold Reports

Before suspicious transaction reports became the international standard, countries with money-laundering prevention systems relied on the analysis of large transactions to detect criminal activity. These reports were often referred to as Currency Transaction Reports (CTR). Large transaction reports are still valued in some jurisdictions as an additional source of data that can yield intelligence and also as a means of reconstructing the "money trail" once suspicious activity is detected and criminal investigations are undertaken. However, having a CTR regime is very IT intensive and requires the requisite IT resources to be efficient. Nevertheless, a number of countries have implemented such a system.

Starting in January 2003, Canada implemented a system under which cash transactions above a specified amount (CAN$10,000) are to be reported to FINTRAC, the Canadian FIU. International wire transfers above the same amount must also be reported. A similar obligation exists in Australia, where cash dealers must report cash transactions to which they are a party involving currency (coin or paper money) of the equivalent of AU$10,000 or more and all international wire transfers.

Analysis of reports

The second element of the core functions of an FIU, following the collection element described above is the analysis of the information received by the FIU. The types of analysis performed by

6 United Nations Convention Against Corruption, Article 14, par. 2

7 A small number of countries monitor all international transactions wire transactions without any threshold
the FIU can be summed up in three categories: tactical analysis, operational analysis and strategic analysis.

**Tactical analysis**

Tactical analysis is the process of the collection of data needed to build a case and the provision of accompanying facts on particular individuals, entities and events to support the case. Tactical analysis is goal orientated. The purpose of analysis is to establish whether the data contained in the reports provides a sufficient basis to warrant transmitting the file for further investigation or for prosecution to the competent authorities. The line that separates the analysis performed by the FIU from the investigations performed by law-enforcement authorities will depend on the type of FIU involved and may also differ for other reasons between jurisdictions.

Though tactical analysis may be performed on all incoming reports, SAR/STR reports are the most likely to provide useful leads in corruption cases. This form of analysis seeks to prove or rule out its association with certain criminal behavior—money laundering or a predicate crime. The analyst forms hypotheses and inferences based on the evaluation and analysis of the data to assist the FIU and/or LEA in identifying activity patterns, new targets, relationships among the suspect and accomplices, investigative leads, criminal profiles, and so on.

Tactical analysis includes the matching of data received from reporting institutions with data held by the FIU or accessible to it, including lists of names, addresses, phone numbers, and data in the other reports forwarded by the reporting entities. For example, the ACA contacted the FIU two years ago about the target of an investigation to determine if the FIU had any intelligence that might support the ACA investigation. The FIU, at that time, did not have any information about the ACA’s target. However, the FIU entered the identifying data, as provided by the ACA, of the target of the ACA investigation into their database. Two years later a reporting entity reports a suspicious transaction report to the FIU about an individual. Through their tactical analysis, the FIU determines that the subject of the STR is a first cousin of the previous target of the aforementioned ACA investigation. The FIU conducts further tactical analysis of the former ACA target of an investigation to determine if there is a nexus between the cousins that might be of interest to the ACA.
Operational Analysis

Operational analysis uses tactical information to formulate different hypotheses on the possible activities of a suspected criminal. It uses all sources of information available to the FIU to produce added value reports. Operational analysis supports the investigative process. It uses all sources of information available to the FIU to produce activity patterns, new targets, relationships among the subject and his or her accomplices, investigative leads, and criminal profiles.

One method operational analysis is called financial profiling or net worth analysis where the analyst develops indicators for concealed income of an individual, a group of individuals, or an organization. This is done by gathering, organizing, and presenting evidence related to the financial status of targets of the analysis indicating that the targets cannot demonstrate a legitimate source for the difference between income and assets/outflow/lifestyle.

Strategic analysis

This is the process of developing knowledge to be used in shaping the work of the FIU in the future. This is not related to individual cases, but rather to new issues and trends. It generally consist of the identification of evolving criminal patterns in a particular group or the provision of
broad insights into emerging patterns of criminality at the national level to support the development of a strategic plan for the FIU.

Questions:
1. What information do you think would be useful to obtain in the tactical analysis of an STR to support the investigation?
2. Does the anti-corruption agency have access to this information, if yes, how does it obtain it?
3. Does the anti-corruption agency feed information to the FIU on new/evolving trends regarding corruption?

Dissemination of information- Relation with other agencies

The third core function of an FIU is the dissemination of the information it has received and the sharing of the results of its analysis. The ability of a FIU to quickly share reliable financial intelligence and related information with domestic and foreign authorities is critical to the success of its mission. Because funds move quickly in and out of financial institutions and across national boundaries, a FIU must be able to provide, as rapidly as possible, its information to competent authorities in order to have an effective anti-money laundering and countering the financing of terrorism regime.

There are three aspects to the dissemination function of FIUs. The first concerns the duty of the FIU to transmit information to the competent authorities for further investigation or prosecution whenever its analysis reveals suspicions of money laundering or other criminal activity. The decision as to which authority will receive the information depends on the legal system of the country involved and the mandate of the respective agencies. In some systems, the information is transmitted to the competent authorities (e.g. Police, Prosecuting authority or ACA, often depending on the suspicions developed during the analysis) so they may carry out the investigations that will result in a file ready to be transmitted to the prosecuting authorities for prosecution. In other systems, the file is transmitted directly to the prosecuting authorities.

The second concerns the exchange of information between the FIU and domestic agencies other than the ones to which files are transmitted for further investigation or prosecution. In determining the agencies that will be authorized to receive financial information from the FIU, legislators must weigh the privacy rights of individuals against the needs of domestic agencies for timely financial information. The FIUs may also be in a position to assist other agencies in the country to accomplish their mission by providing them with useful financial information. Among the main potential recipients of FIU intelligence are financial sector regulators and supervisors, tax authorities, customs and other regulators, to include anti-corruption bodies. The ability of the FIU
to provide this assistance depends on the laws that govern the dissemination of information by the FIU.

The third is the international exchange of information, mainly, but not exclusively, from FIU to FIU, the international FIU-to- FIU network facilitates the rapid exchange of financial intelligence across borders. The EGMONT Secure Web is a prime example of effective and efficient exchange of information between FIUs. An FIU’s ability to share information with its counterparts and other agencies in foreign governments is often determined by law or statute; however, the international standards state that countries should ensure that their competent authorities provide the widest range of international cooperation to their foreign counterparts.

*Dissemination of information*

Below are two examples that illustrate the utility of how collaboration between the FIU and an anti-corruption agency can work together in a financial crime investigation. In one of the case examples, there is collaboration by various competent authorities including an anti-corruption agency and the FIU.
1. Simple Case Example on how an STR/SAR can lead to successful prosecution

A local bank submits an SAR to the national FIU on a customer. The FIU conducts an analysis and sends the report to the local Intelligence Analyst (IA) at the nearest law enforcement agency, investigations office, which has responsibility to investigate possible money laundering offenses in the area where the bank is located.

The local IA runs some routine checks and submits the report to a Special Agent (SA), Criminal Investigator for further investigation (SA). The SA reviews the report and then opens up a case and runs checks on the target of the SAR. These checks include criminal history checks, CTR (Currency Transaction Report) checks, driver license checks, and others. From the initial SAR the SA has the address of the target and other identifying data (date of birth).

The SA goes to the bank and interviews the bank teller that submitted the SAR. The teller advises the SA that the target came into the bank and deposited $8,800 cash into his account. Initially the teller did not think this activity suspicious until she reviewed his account activity while crediting his account and noticed that he had deposited $9,700 in cash the same day at another bank branch located 45 kilometers away. The teller found this activity suspicious and thought the customer might be involved in drug trafficking.

The SA coordinates surveillance of the target with other SAs and discovers five other possible conspirators involved in similar activity, seemingly unemployed and frequenting different bank branches. The SA contacts the local prosecutors’ office and obtains a subpoena to obtain the bank records of the five targets identified by surveillance and other investigative techniques, trash runs, mail covers and interviews. The analysis of the bank records indicates that the group of five is involved in depositing $7,000-$9,900, in cash, two to three times per week into their respective bank accounts. The money is then wire transferred to an account maintained in another bank in Miami, Florida. Collateral investigations conducted by SAs of the Miami office linked the Miami bank account to narcotics traffickers of the Cali, Colombia cartel.

SAs conducted surveillance and used other investigative techniques (mail cover, trash run) in an attempt to link the funds to a Specified Unlawful Act (SUA), illegal narcotics trafficking. SAs were unable to directly link the group of five to any narcotics but had enough evidence to indict them for structuring offenses. One simple STR/SAR led to the indictment and successful prosecution of persons for structuring offenses involved in moving drug money for the Cali cartel.

---

8 This case example is based on an actual investigation, but adopted to suit the purposes of this module.

9 Title 31 of the United States Code, section 5324, provides (in part): “No person shall, for the purpose of evading the reporting requirements of section 5313 (a) or 5325 or any regulation prescribed under any such section, the reporting or record keeping requirements imposed by any order issued under section 5326, or the record keeping requirements imposed by any regulation prescribed under section 21 of the Federal Deposit Insurance Act or section 123 of Public Law 91–508— [...] (3) structure or assist in structuring, or attempt to structure or assist in structuring, any transaction with one or more domestic financial institutions.
2. Example of multi agency collaboration to include ACA and FIU

The organized crime investigate group (OCG) receives information from an informant that a casino operating in the jurisdiction is doing so illegally. Also, media reports have indicated that the same casino has not adhered to the all the requirements to operate legally in the jurisdiction. One media report claims that the casino has not posted the required $3 million bond with the government allowing it to receive a license to operate. The Minister, however, in charge of the ministry with regulatory authority over casinos has publicly announced that the casino is operating legally and has posted the $3 million bond.

The OCG develops enough information to secure a search warrant to be executed on the casino. During the course of the search, OCG discovers that the casino is operating using “two” sets of books. One set is given to regulators (book #1) while the other (book #2) is the actual money flow of the casino. Concurrently, the OCG had requested assistance from the local FIU to help determine if the bond of $3 million had been paid as claimed by the minister. The local FIU was somewhat of a “Hybrid” type and had a task force concept – meaning it had personnel assigned to it from other agencies and regulatory bodies (Tax, Customs, Police, Central Bank, and ACA). The OCG requested the FIU to determine if the $3 million bond had been paid. The FIU determined that the $3 million bond should have been paid to the competent ministry and recorded and maintained at the Central Bank. By having a task force concept, the FIU was able to determine, quickly, that the $3 million bond had not been paid meaning the public statement of the Minister was inaccurate. This information was conveyed to the Director of the ACA and a joint investigation by the ACA and OCG was initiated with support provided by the FIU.

The results of the search of the casino resulted in discovering a journal entry of a suspicious payment ($200,000) from the casino (book #2) to the highest ranking member of one of the most prominent political parties in the jurisdiction. This amount was wire transferred from the casino account to an account linked to the aforementioned politician, but controlled by other persons. The OCG and ACA obtained subpoenas to retrieve bank records of all accounts identified during the course of the investigation. The OCG and ACA requested the assistance of the FIU in examining the accounts because of the FIUs mandate to combat money laundering and terrorism financing and keen expertise in financial analysis.

The analysis of the bank accounts identified hundreds of suspicious cash transactions in one local bank that had not been reported to the FIU by the financial institution. The cash deposits were allegedly made by individuals linked to the aforementioned politician’s political party. However, evidence indicated that one man – “the bag man” actually affected the cash deposits in the bank and he was also a member of the same political party and a close relative of a local wealthy businessman. Intelligence reports held by the FIU and OCG had linked this wealthy businessman to criminal activity.

The OCG and ACA continued their investigation into the casino, the Minister and the political party and some of its members. The FIU and Central Bank conducted compliance inspections of the local bank that had failed to report the suspicious activity. All agencies involved worked closely together and coordinated efforts and shared information.

---

10 This case example is based on an actual investigation, but has been modified and adopted for the purposes of this module.
The OCG was able to close the casino, the ACA was able to develop enough support to force the Minister to resign, the bank was fined and some employees and the “bag man” were charged with criminal offenses. The ACA was able to develop closer ties to the FIU and OCG. The FIU and Central Bank further enhanced their close working relationship and the FIU exhibited its importance and effectiveness by providing support to the ACA and OCG.

Information sharing

As noted in the aforementioned sections analysis, dissemination and information sharing are at the core functions of an FIU. In this context, how can these core functions assist an anti-corruption agency? If the FIU suspects money laundering, the FIU normally has the authority to share, or route, financial information and intelligence to other domestic authorities for investigation or action. FIUs are typically authorized to cooperate and coordinate its actions with the other domestic authorities devoted to the detection, prevention and prosecution of money laundering and terrorist financing and other predicate offenses. The ability of the FIU to provide this assistance depends on the laws that govern the use the FIU can make of the information it obtains. In most systems, the law determines the agencies with which the FIU may share information and the uses the receiving agency or agencies may make of the information.

Once another agency has received information from the FIU, the law governing the agency will normally specify what uses the agency may make of the information. In particular, these laws (for example, the laws governing the conduct of financial regulators) will normally contain strict confidentiality requirements similar to those applying to the FIU and its staff. As a result, the receiving agency will be able to share the received information only to the extent permitted by law.

Countries may grant FIUs the function of providing investigative support to other law enforcement agencies in the course of ongoing investigations on money laundering and sometimes related predicate offenses. In this case, the FIU would be expected to share information and provide assistance with investigative authorities upon request. These powers may entail the exercise of additional powers that would enable the FIU to request additional information from financial institutions or even to carry out investigations, including identifying potential assets, to be frozen, seized, or confiscated. However, many jurisdictions have laws that prohibit investigative agencies from attempting to use the FIU to circumvent the warrant requirement (typically judicial oversight) to obtain banking information (bank secrecy laws).
The main function of an FIU is to analyze suspicious transactions reported by financial institutions and other reporting entities. In order to conduct the appropriate analysis of STR reports, the FIU should have access, direct or indirect, on a timely basis, to the financial, administrative and law enforcement information that it requires to conduct its analysis. FIUs access information available in foreign financial systems through their foreign counterparts. This system of cooperation is often supported by a network of FIUs, known as the Egmont Group. The Egmont Group was created with the goal of overcoming the obstacles to international cooperation and to help address information sharing, to include banking information, and develop harmony between different types of FIUs (administrative, judicial or law enforcement types).


FIUs can be a bridge on behalf of anti-corruption bodies in obtaining information from another jurisdiction through FIU to FIU cooperation. If corruption activities involve assets with international aspects, FIUs typically are able to exchange information with their foreign counterparts considering corruption is a predicate offense for money laundering. A FIU’s participation in the Egmont Group might help facilitate FIU to FIU cooperation and provide opportunities to share knowledge and expertise.

Below is a case that illustrates the FIU to FIU cooperation in assisting an investigation. Although in this example, the subject is drug trafficking, it very well could be corruption.

**Cooperation between French, Spanish and Luxembourg FIUs:**

TRACFIN, the French FIU receives information from one of its reporting entities, a bank of international dimension: the credit card of one of its clients, M. X…, was seized during the execution of a search warrant in the context of a drug trafficking case by the Spanish authorities, the card was given back to the local branch of the Bank by the authorities”.

TRACFIN analyzed the information received, by consulting its internal databases, and found that Mr. X … was known for having changed money a year prior in a French bureau de change and his bank records showed that he travelled to Spain a few days before the search related to drug trafficking operation;

This information was sent by TRACFIN to the Spanish FIU (SEPBLAC);

TRACFIN received a request for assistance from the Luxembourg FIU relating to Mr. Y…, who is French citizen and director of a business. Mr. Y… has deposited on the account of its business 9 million in cash, in pesetas (Spanish currency). The notes were in very bad condition.

Following this request for assistance, TRACFIN investigates and finds out that Mr. Y… is the brother- in- law of Mr. X…;

TRACFIN connects the Spanish and the Luxembourg FIUs on this case… and it was later found out that the cash deposited in Luxembourg was indeed the proceeds of drug trafficking, laundered through the company of Mr. Y…

Source: On file with FPFDI

The diagram below provides an example of the sharing of information between the FIU and other agencies including foreign counterparts.
Countries may also grant their FIU the power to take provisional measures to deal effectively with cases where urgent action is needed. Because the FIU is a crucial governmental point for identifying suspicious transactions, it is logical to grant the FIU provisional powers to preserve assets that might become subject to confiscation. Such measures could include the temporary freezing of assets as well as other measures that restrain any legal disposition of these assets.

Such provisional powers require, however, that the FIU be able to investigate and identify any assets vulnerable to confiscation under the laws against money laundering.\(^\text{11}\)

ACAs are worthy recipients of FIU reports if such reports involve money laundering and the suspected predicate offense is corruption. However, the flow of information should be upstream as well as downstream meaning that ACAs should feed information into FIUs as well as received intelligence reports of ML violations with a nexus to corruption.

International cooperation among prosecutorial and judicial authorities is vital to any framework that hopes to be comprehensive and efficient against money laundering activities. Almost no prosecution of major corruption-related money laundering can succeed without the support of a foreign jurisdiction at one point of the investigation.

\(^{11}\) For more information on this, Modules 4 and 5 will cover this subject matter.
Questions:

1. In your jurisdiction, what law enforcement agencies are involved in a corruption case?
2. What other national agencies would you possibly include in a corruption case?
3. What are the main foreign destinations of proceeds of corruption laundered from your jurisdiction, and how would you cooperate with these jurisdictions?

Developing a Strategy for More Effective Anti-Corruption Agency – FIU Cooperation

The need for comprehensive anti corruption – anti money laundering strategy. The United Nations Convention against Corruption (UNCAC) recognizes reinforces the strong link between corruption and money laundering. The Convention encourages state parties to create effective Financial Intelligence Unit, use of anti money laundering tools, as part of the efforts to prevent, detect, investigate and prosecute corruption. The Convention clearly defines the need for national level anti-corruption and anti money laundering strategy.

A comprehensive strategy should aim at improving effectiveness of corruption investigations by improving exchange of (secure) information from FIUs to Anti-Corruption Agency (ACAs) and vice versa. This is the upstream downstream flow of financial intelligence. Different countries may have different institutional and legal set ups and arrangements facilitating better flow and use of information from FIUs. Some may opt to define working relations in the legal framework, memorandums of understanding (MOU), secondment agreements, some may want to set up working groups or task forces sharing common objectives, some may plan to improve communications by appointing designated officers, organizing regular meetings, or exchanging reports.

The need for operational coordination. In operational terms, at present ACAs and FIUs tend to work in isolation. Anti Money Laundering tools are seldom used to detect corruption; and corruption investigations often involve FIUs at later stages – unfortunately, often too late for the FIU to provide assistance such as a temporary freeze of assets, immediate and direct communication with foreign counterparts and other methods depending on the type of FIU. The problem is sometimes aggravated when ACAs try to recover assets of corrupt officials abroad and do not exhaust mutual assistance avenues before invoking mutual legal assistance requests.

Working together to prevent corruption. ACAs can work together with FIUs to verify the validity of, and monitor assets declared by public officials in asset registries. Corrupt practices may be

---

12 More will be discussed in Module 3 on the subject of cooperation in combating corruption.
deterred when officials are aware that assets declared are being closely monitored, and any suspicious trends will be detected and reported.

In FIU-provided trainings or communicating with commercial banks, banks should be encouraged to increase customer due diligence and to identify typologies and trends related to laundering of corruption proceeds. Banks should be trained to identify Politically Exposed Persons (PEPs) and report suspicious activities to the FIUs, to include domestic PEPs.

*Use of AML tools in detecting corruption.* Some FIUs receive hundreds or thousands of STRs/SARs every day, thus sharing key words or key terms to FIUs which will in turn share to commercial Banks will help them in providing early detection. The government, similar to the case in Mexico, should also develop list of domestic PEPs to be provided to the FIUs so that they can make use of domestic authorities and the international network to monitor movement of assets in the country and abroad. FIUs should also be involved since early stages of investigation in order to help AC authorities to trace and seize assets belonging to suspects.
Summary and Review of Module 2

In this Module we looked at the definition of a financial intelligence unit, namely, that it is a central national agency that receives analyses and disseminates financial intelligence information. We further observed that they are different types of FIUs that are established by various jurisdictions. This diversity is dependent on the legal, political and economic history of a jurisdiction.

However, we did observe that each type of FIU has its advantages and disadvantages and a jurisdiction will have to determine what is best for it taking into account its history and need.

Generally, as discussed in this module, the FIU’s role is to conduct analysis of information it receives from reporting entities and package it in a manner that is of value to investigative bodies. We noted that the information should be such that it can be transformed into evidence that can be used to investigate, prosecute and ultimately convict a person who is alleged to be involved in criminal activities.

We highlighted the ability of the FIU to provide assistance to other agencies depends on the laws that govern the use the FIU can make of the information it obtains. We noted that in most systems, the law determines the agencies with which the FIU may share information and the uses the receiving agency or agencies may make of the information.

We ended the module by observing the need for anti-corruption agencies to cooperate with FIUs in corruption investigations. We looked at two illustrative cases that elaborate on this subject matter to show that the FIU can indeed play a role in assisting anti-corruption agencies in their efforts to fight corruption. More of this issue will be discussed further in Module 3.