Asia-Pacific
Economic Cooperation

Best Practices in Investigating and Prosecuting Corruption

Using Financial Flow Tracking Techniques and Financial Intelligence

A Handbook

APEC Anticorruption and Transparency Working Group (ACTWG)

September 2015

TABLE OF CONTENTS

PRESENTATION

This handbook was elaborated under the scope of APEC project M SCE 01 12A-1: "Capacity Building Workshops on Designing Best Models on Prosecuting Corruption and Money Laundering Cases Using Financial Flow Tracking Techniques and Investigative Intelligence for Effective Conviction and Asset Recovery to Promote Regional Economic Integration".[1] The project was born within the APEC Anticorruption and Transparency Working Group (ACTWG), from joined efforts made by Chile and Thailand to improve the investigation and prosecution of corruption and money laundering. Both economies, members of the APEC ACTWG, led the project under the Multi Year Project APEC Guidelines, between 2013 and 2015.

This multi-year effort was designed in two subsequent stages.

The first stage, led by Chile, consisted of the revision of the legislative and regulatory framework for investigating and prosecuting corruption and the laundering of its proceeds of 10 APEC economies: Australia; Canada; Chile; Indonesia; Hong Kong, China; Malaysia; Mexico; Peru; The Russian Federation; and The United States. Those economies – with the exception of Canada –, plus Brunei Darussalam; Chinese Taipei; The Republic of the Philippines; and Viet Nam participated in a three-day workshop which took place in Santiago de Chile from June 11 to June 13, 2013. During the workshop, the economies presented and discussed their best practices for investigating and prosecuting corruption and the laundering of its proceeds.

The objectives of the workshop were to focus the presentations on financial investigation techniques and on the use of digital forensics for uncovering corruption. The presentations, however, also brought to the table other important issues in investigating corruption, such as the essential elements for building an investigation plan and strategy and the best practices related to building coordination mechanisms and cooperative networks both domestically and internationally.

Chapters I to V of this Handbook capture the knowledge gained from this workshop, including the content of the presentations and discussions developed therein.

We start by introducing the basics of any investigation: how to develop a plan, how to organize the resources, identify potential targets, define the scope of the investigation and select the techniques that will be used to potentially prove the allegations (Chapter I).

Chapter II focuses on issues of coordination, both domestic and international, and on the related aspect of building cooperative networks. We review the best practices for domestic cooperation, taking into account the internationally recognized practices for sharing information, especially financial information. In light of the workshop discussions, we specifically revisited the coordination between FIUs and other law enforcement agencies.

While Chapter III focuses on the gathering of peripheral evidence, through open sources techniques, database searches, and digital forensics tools, Chapter IV explains the gathering of private sources of evidence, including the use of digital forensic tools. Chapter V provides a practical approach on how to perform human intelligence, specifically the technique of profiling suspects.

The second stage of the project, led by Thailand, consisted of a workshop that took place in Pattaya from September 22 to September 24, 2014. During the workshop, the attending APEC economies shared best practices for the gathering of financial evidence and the recovery of the proceeds of corruption. Furthermore, the workshop aimed to highlight current developments in asset tracing, freezing, seizure, confiscation and repatriation issues through the examination of recent case examples, operational approaches, the use of new technologies and coordinating strategies.

Chapters VI to X of the handbook were elaborated through a process similar to that of the first part: knowledge gained from the 2014 workshop in Thailand, the content of the presentations and the discussions developed therein served as a basis for the writing of its chapters.

These chapters, on the one hand, complete the evidence gathering chapters, mainly by focusing on the gathering of financial evidence (Chapter VI). On the other hand, they develop the asset recovery process in four chapters. Chapter VII focuses on restraining measures encompassing the provisional freezing and seizure of assets, on the different types of restraining orders (person or asset directed), and on obtaining freezing orders from another economy and enforcing foreign restraining orders. Chapter VIII explains how the assets are managed after seizure according to the type of asset, the powers and duties of the asset manager and best practices for handling practical issues, such as expenses or use of restrained assets. Chapter IX focuses on the methods of confiscation, the different confiscation proceedings, the disposal of confiscated assets, and it also addresses potential substitutes for confiscation, such as fines and disgorgement of profits. Chapter X closes this handbook with a general explanation of

the best practices related to the repatriation of the confiscated assets to the member economy of origin.

CHAPTER I. PRE-CONDITIONS FOR CONDUCTING COMPLEX INVESTIGATIONS

Investigations of corruption are often very complex, since they usually involve a multitude of relevant actors and targets, movement of assets and financial vehicles used or placed in overseas jurisdictions. Successful investigations of complex corruption schemes are not only the result of dedicated individual efforts but also the consequence of some institutional pre-requisites, which provide an adequate environment for such a success to take place.

This introductory Chapter is devoted to recalling the essential pre-conditions that any competent authority needs to envisage as the ideal grounds for ensuring the success of complex investigations and, to the extent of its responsibilities, help to build the institutional capacities towards its fulfillment.

The primary objectives of an investigation are:

- Evidence gathering
- Fact finding and reconstruction
- Reporting to / supporting conclusions of the competent authorities.

The investigative team's main responsibility is to bring facts to life for prosecutors, judges and other competent authorities with decision-making capacities. Investigations should be capable of providing grounds to both criminal prosecutions and to the reorganization of public or private administrations with the purpose of preventing the same facts from happening again.

The first step of an effective investigation is its planning. Investigators should begin by identifying the standards, rules, and procedures that govern the circumstances under investigation and the information already available. They must determine what additional information will be required before findings and recommendations may be made to the competent authority, and therefore should elaborate an understanding of the steps which are required to obtain the necessary evidence, including, among others, a list of potential sources of information and specific strategies for witnesses interviewing, in order to reach a conclusion on the merits. The plan should also try to anticipate possible factual and legal challenges and build a case to avoid them.

A policy document including a clear description of the facts that gave rise to the investigation, existent evidence and strategies for gathering additional information, as well as all decisions made in the different investigative stages, along with their justification, is a helpful tool for the investigative team to plan the different steps of the investigation and progressively re-evaluate such plans against evolving developments in an ongoing manner.

The key elements of an investigation plan are the following:

A. Ensuring adequate resources

Before starting an investigation it is important to properly evaluate the resources that will be necessary to complete the task. A comprehensive list of all the needed resources for the investigation to be successful -either human, financial or material-, is a relevant initial step to organize the investigative work from the beginning.[2]

Basic items to be factored in are whether and what types of internal and/or external expertise should be involved with the investigative team; the special investigative techniques that will be required and their potential costs; whether interagency cooperation/coordination will be necessary, and appropriate paths to ensure it, including the use of international legal or operational cooperation, information exchange and possible travel; and the usefulness of establishing joint investigative teams.

As many member economies recognized, from the onset of any investigation particular consideration should be given to the necessary expertise to trace financial flows and other illicitly acquired assets, especially when other jurisdictions are identified as potential recipients of the proceeds of the crime.

Finally, it is also essential to ensure the confidentiality of the investigation and its products and, in turn, evaluate whether the systems for the creation, retention and analysis of records fulfill this condition.

B. Building an investigation team

1. Team selection

The selection of an effective team is crucial to the success of an investigation. Team members should possess specific investigative skills likely to be needed in the investigation. An increasing number of member economies are aware of the need to

ensure an adequate number of properly trained financial investigators, in addition to more traditional field or legal investigators.

Necessary skills to conduct large-scale corruption investigations include financial investigations and information technology skills, knowledge of international conventions, standards, and international cooperation mechanisms, specific expertise in undercover and surveillance operations, proper experience in interviewing and witness preparation, and the ability to analyze intelligence. Report writing capacities are also essential.

Team members must be aware of all the implications of the investigation, particularly when undercover work is to be conducted.[3]

Finally, it is also essential that the integrity of the team members is absolutely ensured and, to this end, the background of investigators should be thoroughly checked, including social and family ties and lifestyles.

2. Team training

Adequate training and resources for investigators are necessary to ensure that reported cases are dealt with effectively; the wide range of corruption types requires an equally wide range of skills and knowledge on the part of investigators.

Training and education programs should be standardized within each competent authority. Basic training should be envisaged at entry level, and specialized training for select officers should be conducted at both entry level and throughout the investigator's career. Investigators' training may also be aligned with training for specialist prosecutors and other relevant enforcement authorities.

It has been internationally advised that the formal selection of the investigation team members should be followed by formal instruction in at least three primary disciplines: financial intelligence, evidence gathering, and asset tracing/freezing. Further training should be given for purposes of money laundering investigations, enhanced financial intelligence, and criminal and non-conviction based confiscation.[4]

Since these investigations are usually complex and lengthy, financial investigators, intelligence analysts and other authorities should be trained in how to periodically document their findings and in the skills of report writing. Reports are an integral part of financial investigations: the ability to convey concepts, findings and conclusions in a clear, concise and informative manner is essential to their success and therefore it is highly advisable that member economies dedicate the necessary resources to this end.

Where possible, training should not be exclusive to law enforcement but also include such sectors that are required to report suspicious or risky activity. It may also include multiple jurisdictions in order to allow for best practices sharing, learning comparative models and enhancing co-operation. Besides, investigators should remain vigilant in staying current to new trends and typologies. To these ends, APEC economies should encourage their investigators to attend regional and international training workshops with their foreign counterparts.

For example, Chile's Specialized Anticorruption Unit (*Unidad Especializada Anticorrupción* – UNAC) organizes periodic training activities coordinated by specialized lawyers who educate and update prosecutors, investigation agencies and other actors on anticorruption and financial investigations.

3. Engaging specialized experts

Most times, the availability of enough skilled and trained investigators depends on whether enough resources are available for law enforcement. As resources are usually limited, training investigators in the sophisticated techniques needed to deal with the complexities of large-scale corruption cases represents a particular challenge. In such scenarios, engaging experts is convenient to enhance the team's level of expertise.

Specialized experts can play a significant role in financial investigations, e.g. regarding financial analysis, forensic accounting, and computer forensics. Experts use IT tools for tracking and analyzing data and other evidence, and explain transactions or how specific industries or business work.

In particular, assistance of forensic accountants should always be available to the financial investigation team: an opinion derived from a forensic test may help to obtain additional information or may provide closure to other areas of the inquiry, assist in tracing transactions back to the money or assets, provide full analytical review of money flows, identify unexplained transactions, match employees' lifestyle with predicted income, or establish links between related parties.

There are various models of drawing on specialized expertise. In some member economies, anti-corruption investigation and prosecution authorities try to build-up their own in-house expertise on specific subject matters, like the US Department of Justice does with forensic accountants or Chile with their in-house financial analysts. Other economies, often those of more limited resources, opt for the involvement of external expertise or a combination of the two approaches. When engaging private entities,

however, adequate safeguards should be in place to minimize the risks of compromising the integrity of investigations.

C. Identifying potential targets

Embezzlement of public funds and corruption cases always involve personal gains. From the criminal perspective, an important part of keeping the crime uncovered is to bring satisfactory benefits for all those included in the scheme, in order to ensure their commitment to secrecy. Therefore, in order to identify potential targets of the investigation it is important to "follow the money" or other forms of gain or benefits, and determine who profited from the corrupt act and how. To such end, the following suggestions should be taken into account: [5]

- Tax returns, financial disclosure forms, employment records, and loan applications should be reviewed;
- Immediate superiors and fellow employees are usually good sources of information (suspects have a way of revealing themselves and their processes to those they associate with on a daily basis);
- Public registries, credit card accounts, expensive celebrations, school fees and support measures for children, foreign bank accounts, homes and second houses and holiday homes should be located and assessed, as well as means of transport and employees' salaries and perks;
- Even at these preliminary stages, experts should be on hand for consultation, even in an informal fashion. Document examiners, for example, can be consulted for handwriting examinations, signatures, paper and ink analysis and comparison, erasures or substitution of documents, and restoration of obliterated writing. Fingerprint experts, experts in computers and cybercrimes (e-commerce fraud, stenography analysis, data recovery, etc.) and experts in DNA testing (for intimate contact items, such as used stamps and envelopes) may be of great help.
- Once a particular suspect has been identified (or grounds for suspicions arise), the screening process should include persons with whom they have strong ties (family members, business associates, etc.) considering that bank accounts, real estate, land or stocks are often in the names of people of the suspect's trust.

D. Developing an investigative strategy

1. Case selection strategies

Given the extent of corruption, the range of cases likely to exist, the variety of possible outcomes, and the limits imposed by human and financial resource constraints, most anticorruption law enforcement agencies will find it necessary to make priority choices as to the cases to pursue, and the outcomes to seek. In practice, it must be recognized that not every suspected case can be fully investigated and prosecuted.

Moreover, as it has been widely recognized, detecting corruption involves a key problem in itself. Although decidedly not a "victimless" crime, many crimes of corruption, particularly bribery and trading in influence, are consensual crimes and therefore complainants are hard to find. Furthermore, as corrupt deals usually occurred without witnesses, rarely are documented and are normally surrounded by secrecy, few overt occurrences are likely to be reported by witnesses, unless they are "insiders". The importance of intelligence in the pro-active detection of corruption therefore stands out. Anticorruption agencies that only rely on reactive strategies are usually overloaded by thousands of small cases which, coupled with inappropriate case-management techniques, transform them in heavily bureaucratic agencies with the obvious loss of social legitimacy in the long run[6].

Even though it is usually delimited by law or by specific agency guidelines, prioritizing involves the exercise of considerable discretion, so it must be managed carefully to ensure consistency, transparency and the credibility of both the decision-making process and its outcomes. A major element in this regard is the setting and, where appropriate, the publication of criteria for case selection (sometimes referred to as a prosecution policy paper). This document can help reassure those who make complaints, as well as the general public that a decision not to pursue a particular reported case is based on objective criteria and not on improper motives.

Case selection criteria should include the following:[7]

- **The seriousness and prevalence of the alleged offense**

Assuming that the fundamental objective of an anti-corruption strategy is to reduce overall corruption, priority may be given to cases that involve the most common forms of corruption. Where large numbers of individuals are involved, or structural practices are targeted, the case will often lead to proactive remedial outcomes such as the setting of new ethical standards or the training of public officials, general preventive policies with large-scale remedial capabilities.

On the other hand, as overall expertise and knowledge are gained and greater numbers of cases are dealt with, intelligence information can be gathered and assessed, constituting a useful tool for prioritizing cases on the grounds of their seriousness. Intelligence should guide case selection decision making processes through the detection of overall corruption patterns and the identification of such cases which are causing the most social or economic harm.

- **Related cases in the past to establish precedent**

Priority can be given to cases that raise social, political or legal issues the results of which can be applied to many future cases. Examples include dealing publicly with common conduct not hitherto perceived as being corrupt in order to change public perceptions, and cases that test the scope of criminal corruption offences so that they either set a useful legal precedent or establish the need for legislation to close a legal gap.

- **The viability or probability of a satisfactory outcome**

Cases may be downgraded or deferred if an initial review establishes that no satisfactory outcome can be achieved. Examples include cases in which the only desirable outcome is a criminal prosecution although it may not be possible or in the public interest to prosecute (i.e. the suspect has died or disappeared, is already serving a lengthy term in prison, is extremely old or critically ill) or where essential evidence has been lost. The assessment of such cases should include a review of whether other appropriate remedies may be available.

- **The availability of financial, human, and/or technical resources to adequately investigate and prosecute**

The overall availability of resources is always a concern in determining how many cases can be dealt with at the same time or within a given time period. An assessment of costs and benefits before decisions are made is thus important. In cases of grand corruption and with transnational implications there can be substantial costs in areas such as travel and foreign legal services, but the public interest may demand that examples are made of corrupt senior officials for reasons of deterrence and credibility, to recover large proceeds hidden either at home or abroad and to restore faith in government.

A periodic reassessment of caseloads is required, since the burden of particular cases tends to fluctuate as investigations proceed. A single major case, if pursued, may result

in the effective deferral of large numbers of minor cases, and the unavailability of specialist expertise may make specific cases temporarily impossible to pursue.

- **The legal nature of the alleged corrupt activity**

Corruption can give place to either criminal or administrative/civil procedures. The nature of the offence will often determine which agency is competent to deal with it. The possibility of initiating action other than a prosecution, if circumstances allow, should be considered taking into account the criteria referred to here and the prosecution agencies' workload, among other factors.

2. Case management

Member economies should be proactive in developing effective and efficient strategies to make financial investigations an operational part of their law enforcement efforts. Although some corruption cases may be simple and straightforward, with witnesses and evidence readily available,[8] in most cases –especially where corruption is systemic– the challenge is one of volume. Serious corruption investigations, particularly those involving high-level or grand corruption, can be highly time-consuming, complex and expensive.

To ensure the efficient use of resources and successful outcomes, the investigative tools and personnel involved must be managed effectively. The work of the investigative team should be conducted in accordance with an agreed strategy and supervised by an investigative manager in charge of receiving information about the progress of investigators regularly.[9]

Key elements that will facilitate case management include:

- Periodically conducting needs assessments and promoting proper allocation of resources.
- Articulating clear objectives for relevant departments and agencies that include effective coordinating structures and accountability.
- Establishing strategic planning working groups to develop an effective policy that incorporates the skills of all relevant agencies into an action plan; these groups should include representatives from all relevant agencies and components participating in financial investigations.
- Creating specialized investigative units focusing on financial investigations and asset tracing/freezing.

When managing a case, the sequencing of actions can be of the greatest importance. For instance, measures that pose a risk of disclosing to outsiders the existence of the investigation and, to some degree, its purpose (such as the interviewing of witnesses and the conducting of search and seizure operations) should not be undertaken until after other measures have been taken, as they will only be effective if the target has not been alerted. Besides, some procedures may become urgent if it appears that evidence could be destroyed or illicit proceeds might be moved.[10]

Investigative teams may be assigned to specific target individuals, or focus exclusively on particular aspects of the case in complex investigations. For example, one group might be engaged in the tracing of proceeds, while others interview witnesses or maintain suspects' surveillance.

Table 1: Managing transnational or "Grand Corruption cases"[11]

Cases involving "grand corruption" or that have significant transnational aspects raise additional management issues. For example, cases where high level officials are suspected raise exceptional concerns about integrity and security and are likely to attract extensive media attention. Large-scale and sophisticated corruption is well resourced and well connected; making it more likely that conventional sources of information will either not have the necessary information or evidence or be afraid to cooperate. Senior officials may be in a position to interfere with investigations. The magnitude of proceeds in grand corruption cases makes it more likely that part of the overall case strategy is the tracing and forfeiture of the proceeds, and where they have been transferred abroad, obtaining their return. Allegations that senior officials are corrupt may also be extremely damaging in personal and political terms if they become public and later turn out to be unsubstantiated or false.

Transnational elements are more likely to arise in grand corruption cases. Senior officials realize that there is no domestic shelter for the proceeds while they are in office and generally transfer very large sums abroad, where they are invested or concealed. In many cases, the corruption itself has foreign elements, such as the bribery of officials by foreign companies seeking Government contracts or the avoidance of costly domestic legal standards in areas such as employment or environmental protection. The offenders themselves also often maintain foreign residences and flee there once an investigation becomes apparent.

Generally, transnational or multinational investigations require much the same coordination as do major domestic cases, but the coordination and management must be accomplished by various law enforcement agencies that report to sovereign Governments which have a potentially wide range of political and criminal justice agendas.

Coordination will usually involve liaison between officials at more senior levels and

their foreign counterparts to set overall priorities and agendas, and more direct cooperation among investigators within the criteria set out for them. From a substantive standpoint, investigative teams in such cases will generally be much larger and will involve additional areas of specialization such as extradition, mutual legal assistance and international money laundering.

E. Choosing investigative methods and techniques

Determining which investigative tools to use depends on a variety of factors, including the nature of the alleged violations and the available resources.

In the course of the investigation, it is a normal progression to go from investigative measures that do not alert the targets that they are under investigation –research of public databases, collection of public information, informal interviews of potential witnesses that are not close connected with the targets, etc. - to measures that, once taken, allow the investigators to secure both evidences and proceeds of the crime. In other words, investigators must first arm themselves with as much information as possible to both ensure that potential witnesses –and, where admissible, defendants- tell the truth, and also keep criminal proceeds from dissipating because the investigation becomes public.

The following paragraphs classify some of the investigative techniques used by several APEC economies in standard and complex or special investigative techniques. The following Chapters will specifically focus on the gathering of peripheral, digital and human evidence.

1. Standard investigative techniques

Interviewing witnesses and defendants

Conducting interviews is one of the techniques for investigators to gather evidence and information in furtherance of their financial investigation. Interviews with potential witnesses or suspects –for those member economies where cooperation of suspects might be exchanged by leniency– however, should not commence before considering the potential negative impact on the investigation by soliciting the witness's co-operation. Even if not required by the criminal procedure rules, detailed reports of investigation should be completed to document interview results. Interview reports may be helpful in refreshing investigators and witnesses' recollections of events during criminal or civil formal legal proceedings.

Still, the investigator should by no means be satisfied with interviews as a sole piece of evidence. Testimonies and facts recollected through informal interviews shall be tried to be re-confirmed through all other legal means of obtaining evidence to overcome the

presumption of innocence.

Physical Surveillance
This is a useful technique to gain general background and intelligence on individuals/businesses, habits and relationships of suspects. It may also include electronic surveillance, through the use of visual surveillance in public places with the use of photography, video recording, optical and radio devices. Surveillance can be especially useful in financial investigations in cases involving the movement of bulk currency and by identifying "gatekeepers" involved in the development and implementation of ML schemes. Surveillance of targets can often identify where financial and related records might be stored and lead to the discovery of assets. In addition, surveillance can help corroborate financial data and identify other targets and associates.
Trash runs
They consist of searching the suspect's discarded trash for evidence. It can be an effective way of obtaining leads as to where assets are maintained, as well as help develop probable cause for more coercive measures and evidence for use at trial. Suspects frequently discard evidence, including financial records and correspondence that may be valuable to a financial investigation.
Searches and other compulsory measures to obtain evidence
These measures should be used to gather evidence of criminal activity that cannot be obtained by other means without authorization from a competent authority. The timely use of these powers to obtain evidence minimizes the opportunity for suspects to purge records and/or destroy evidence. In addition to seizing paper documentation, investigators should intercept or seize information from computers and other electronic devices, such as telephone, fax, e-mail, mail, public or private networks. The execution of these powers should always be properly planned and be lawfully conducted in accordance with existing policies and procedures.

2. Special investigative techniques

Although investigators of corruption cases tend to rely heavily on basic investigative techniques, good practice shows that more focus should be given to the use of special investigative techniques, financial investigations and international cooperation for the successful investigation and prosecution of complex and cross-border corruption crimes.

Special investigative techniques are applied by competent judicial, prosecuting and investigating authorities in the context of criminal investigations for the purpose of

detecting and investigating complex criminality, in order to gather information in such a way as not to alert the target persons.[12]

Special investigative techniques, although effective, entail serious risks that should be adequately addressed. Member economies should ensure: that their competent authorities are properly trained in using these techniques, that clear policy and procedural guidelines are established and followed, and that proper operational oversight is conducted at the managerial level.

The following techniques have proven useful in corruption and financial investigations:[13]

Intercepting communications

Electronic surveillance techniques, such as electronic intercepts of wire, oral communications, electronic media and the use of tracking devices, can be very useful in financial investigations. This technique can help identify co-conspirators, provide insight into the operations of the criminal organization, provide real time information/evidence that can be acted upon using other investigative techniques and can lead to the discovery of assets, financial records and other evidence. Competent authorities should be trained in these techniques in accordance with the basic principles of their domestic laws.

Controlled delivery

This is an effective investigative technique involving the transportation of contraband, currency, or monetary instruments to suspected violators under the control of law enforcement officers. Cross-border controlled deliveries can be performed in cooperation with customs and other foreign competent authorities, or on the basis of international agreements. Controlled deliveries are conducted to:

- Disrupt and dismantle criminal organizations engaged in smuggling contraband, currency, or monetary instruments across borders.
- Broaden the scope of an investigation, identify additional and higher level violators, and obtain further evidence.
- Establish evidentiary proof that the suspects were knowingly in possession of contraband or currency.
- Identify the violator's assets for consideration in asset forfeiture proceedings.

Cross-border observation

This investigative technique allows keeping a person who is located in a foreign

economy under observation, with the authorization of the competent authorities of such economy. It may be used to keep under observation a person to which extradition may apply, or a third person who will probably lead to the offender.

Undercover operation

Undercover operations typically allow investigators access to key evidence that cannot be obtained through other means. An undercover operation is an investigative technique in which a law enforcement officer or a person cooperating with the competent authority, under the direction of a law enforcement authority, takes undercover action to gain evidence or information (e.g. by infiltration of an officer under false identity into a criminal group). This technique includes the use of undercover companies (*i.e.* the use of an enterprise or an organization created to disguise identity or affiliation of individuals, premises and vehicles of operative units), informants (*i.e.* voluntary confidential cooperation with individuals to obtain information about crimes being plotted or already committed; informants can operate openly or secretly, free of charge or for a fee, can be hired as permanent or non-permanent staff) and use of agents *provocateur* or integrity testing (*i.e.* an investigator or other agent acting undercover to entice or provoke another person to commit an illegal act).

Properly conducting undercover operations often requires substantial resources, extensive training and significant preparatory work. The resources it requires, the unique and diverse skill sets it demands and its inherent risks typically make this technique a last resort – normally after other investigative techniques have been unsuccessful. Various significant factors should be considered when envisaging an undercover operation, including the legal framework, whether positive results are actually likely to be achieved, and the reliability of the informants under use.

Given the inherent risk with this technique, undercover operations proposals should be *reviewed and authorized* by designated officials from the competent law enforcement authorities. These officials should be knowledgeable on all aspects of undercover operations. Moreover, the proposal should indicate that traditional investigative techniques have been utilized and have been largely unsuccessful and that the undercover operation is likely the only technique available to gather evidence of the suspected criminal activity. Only highly trained undercover agents should be used in undercover operations.

Undercover operations should be re-evaluated in an ongoing manner, and investigators should always be prepared for its termination. Termination criteria should be established in advance.

The actions performed by law enforcement during undercover operations should be in accordance with the basic principles of existing laws, policies and procedures, and all undercover officers should be highly trained before engaging in such operations.

CHAPTER II. BUILDING COORDINATION AND COOPERATION NETWORKS

The previous Chapter stresses the importance of ensuring adequate resources for an investigation and, among them, human resources. Selection of personnel, training and building trust exercises were pointed out as key pre-conditions for a successful team building strategy.

In all member economies, nonetheless, these human resources are usually distributed in an array of different public agencies and, sometimes, in the private sector. Therefore, rarely can anticorruption units build an internal team that satisfies all the skill requirements. More often, it is necessary to resort to counterparts in other agencies, such as tax agencies, customs, financial intelligence units (FIUs), supervisors of the banking, insurance and securities sectors, public procurement agencies, etc. Liaising with such agencies is usually subjected to both legal and practical challenges of coordination and cooperation.

This Chapter captures the best practices member economies have resorted to in order to overcome these challenges, in particular when engaging with FIUs at the domestic level (Section B) and with foreign counterparts of a different nature (Section C).

A. Internal cooperation and coordination issues

The creation of institutional conditions that ensure that investigative specialized units can work closely with different competent authorities is fundamental for successful investigations. For example, information from tax authorities, oversight institutions, or FIUs can help tracing assets that may have been derived from corruption. Mechanisms that have been stressed for the promotion of intra and inter-agency cooperation include:[14]

- Establishing information sharing systems whereby all investigative services would be aware of previous or on-going investigations made on the same persons and/or legal entities so as to avoid replication.
- Establishing policies and procedures that promote the sharing of information/intelligence within intra-agency and inter-agency cooperative frameworks; such policies and procedures should promote the strategic sharing of the necessary information.

- Establishing a process whereby intra-agency or inter-agency disputes are resolved in the best interest of the investigation.
- Establishing written agreements such as Memorandums of Understanding (MoUs) between agencies to formalize these processes.

Given the need for autonomy and independence on the part of investigators, and taking into account the extreme sensitivity of many corruption cases, care must always be taken when establishing relationships between anticorruption bodies and other government agencies (e.g. internal inspection and audit within government agencies), especially in environments where corruption is believed to be widespread.

Table 2: Multi-disciplinary groups or task forces

SOURCE**:** FATF Report. Operational Issues. Financial Investigations Guidance, June 2012, p**. 17-19**

Particularly in large and complex financial investigations, it is important to assemble a multidisciplinary group or task force to ensure the effective handling of the investigation, prosecution and eventual confiscation. There should be a strategic approach to intra-agency and inter-agency cooperation in an effort to support information/intelligence sharing within and between agencies and with foreign counterparts.

Multi-disciplinary groups or task forces serve to integrate information from different law enforcement and intelligence sources, which had previously been separated by organizational and technical boundaries. In some jurisdictions this requires changes in laws and regulations or may require formalized agreements such as Memorandums of Understanding (MoUs). These task forces leverage existing technologies and develop new technologies in order to provide cross-agency integration and analysis of various forms of data. Furthermore, this information is stored in centralized databases so that any future investigation of any new target of a participating task-force agency can be cross-referenced against that historical data.

Multi-disciplinary groups may comprise a range of individuals, including specialized financial investigators, experts in financial analysis, forensic accountants, forensic computer specialists, prosecutors, and asset managers. Experts may be appointed or seconded from other agencies, such as a regulatory authority, the FIU, a tax authority, an auditing agency, the office of an inspector general, or even drawn from the private sector on an as-needed basis. The multi-disciplinary groups should include individuals with the expertise necessary to analyze significant volumes of financial, banking, business and accounting documents, including wire transfers, financial statements and 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 such investigative techniques as undercover operations, intercepting communications, accessing computer systems, and controlled

delivery. Multi-disciplinary groups should also consist of criminal investigators who have the necessary knowledge and experience in effectively using traditional investigative techniques. Prosecutors also require similar expertise and experience to effectively present the case in court.

B. Collaboration between law enforcement agencies and FIUs

Together with intelligence divisions of law enforcement and other competent authorities, Financial Intelligence Units (FIUs) are one of the competent authorities that can initiate or enhance financial investigations. Financial intelligence received by these agencies should be thoroughly analyzed and, expectedly, result in the proactive initiation of money laundering investigations.

The Egmont Group defines a FIU as 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 and potential financing of terrorism; or (ii) required by national legislation or regulation, in order to counter money laundering and terrorism financing.[15]

A core function of FIUs is to analyze the information they collect and to disseminate the results of such analysis through competent enforcement authorities. FIU's analytical capabilities allow them to develop different intelligence products that can be useful to investigative authorities.

Member economies are free to establish their FIUs within the branch of the Government of their preference. In fact, around the world, there have been identified four institutional structures of FIUs:

- The judicial model of FIU is established within the judicial branch of government.
- The law enforcement model of FIU works in support of other law enforcement and judicial agencies. It may have concurrent or even competing investigative capacities over money laundering.
- The administrative model of FIU is a centralized, independent, administrative authority, which receives and processes information from the designated parties and transmits it, when deemed appropriate, to law enforcement or judicial authorities for prosecution.
- Hybrid models of FIU combine elements of at least two of the previous FIU models.

A modern FIU can provide a range of services to anti-corruption and law enforcement agencies. These services range from simple data descriptions to complex analysis, including:

- scalable link analysis and spatial analysis of geographical locations and interactions
- text mining to find themes and concepts in unstructured data, and
- modeling to develop rules to explain and predict behavior.

Table 3: Best practices

Australia - 2010 "fusion project": Integration or 'fusion' of intelligence and investigative resources to develop the big picture of serious organised crime and corruption.

SOURCE: "The value of a multi-agency approach to detect, analyze and disrupt illicit financial flows", presentation by Mr. Adam Coin, Chargé d'Affaires, Australian Embassy, Santiago de Chile, at the APEC Anti-Corruption and Transparency Working Group (ACTWG), *Capacity Building Workshops on Designing Best Models on Prosecuting Corruption and Money Laundering Cases Using Financial Flow Tracking Techniques and Investigative Intelligence for Effective Conviction and Asset Recovery to Promote Regional Economic Integration*, Santiago, Chile, 11-13 June 2013.

The purpose of fusion is to help Australian law enforcement agencies to see the bigger picture of organised and transnational crime. The bigger picture can't be seen if information and intelligence remains separated in multiple agencies. Fusion is the process of integrating and analysing those multiple sources. So far, the project has informed the design of various initiatives, including the Counter-Terrorism Control Centre and the Criminal Assets Confiscation Taskforce. Plans are also underway to establish the Australian Cyber Security Centre.

The Australian Crime Commission Fusion Centre brings together specialists from different government agencies, and different levels of government, with access to multiple information and intelligence holdings. The Fusion Centre includes staff from the Australian intelligence community, the Australian Crime Commission, the Australian Taxation Office, Australia's financial intelligence unit (AUSTRAC), the national welfare agency (Centrelink), the Department of Immigration and Citizenship, and law enforcement agencies. Staff from these diverse agencies bring expertise in financial investigation, operational psychology, data-mining, statistical analysis, database management and architecture. They put the pieces together from different agencies to produce a more comprehensive picture of criminal targets, risks, threats and vulnerabilities.

Although only established in 2010, the benefits of the project are already apparent. For example, in early 2013, fusion intelligence detected a series of suspicious international transactions from Australia valued in excess of $A20 million. Intelligence also showed the use of false identities and credit cards. Following this detection, Australian law

enforcement agencies located two significant methyl amphetamine laboratories.

Fusion has also paid dividends for the detection of international money laundering and the recovery of assets. For example, in late 2012, fusion identified likely proceeds of crime in excess of $38 million being transferred to a foreign jurisdiction. In another investigation, significant money laundering involving profession facilitators was identified. These detections are now being investigated.

1. Accessibility of FIU disclosures in financial investigations

Financial disclosures and FIU analysis are a valuable source of information. AML/CFT disclosures of reporting entities, whether suspicious transaction reports (STRs) or systematic information required by AML/CFT legislation, can help investigators connect other pieces of information, provide information on where the proceeds of criminal activity are located and when and where these funds are moved.

Effective financial investigations are thus characterized by extensive law enforcement use of FIU information and exchanges of information and personnel. Investigative authorities should be able to ask the FIU for relevant information they may hold when conducting lawful investigations and FIUs should be able to respond to information requests from competent authorities.[16]

Requesting all relevant FIU information should be a basic step in a financial investigation. This should be included as part of a routine investigator "checklist." Therefore, it is essential that investigators have timely access to financial disclosures filed in their jurisdictions. This access does not have to be direct but should be prompt so as to facilitate the incorporation of significant and relevant findings and to further active investigations. Some member economies provide their investigative authorities with direct –although restricted– access to the FIU's database, being able to directly query such database under certain circumstances. Arrangements for investigators' access to the FIU's database should take into consideration information handling issues such as confidentiality, privacy and data protection as well as the respect for international human rights individual rights.

Finally, the FIU will hold, or have access to its own information and information gathered from third parties (both domestic and foreign) that can enhance investigations if provided at the request of the investigative authorities. FIUs responses to specific requests can support existing activity by identifying and locating proceeds of crime and supply information, which can assist in securing convictions and confiscations. Some of this information will be confidential or sensitive, and the manner in which it can be

shared may be restricted. Restrictions may be imposed by law or by the third party originator of the information. Thus, when receiving information from the FIU, investigators should note the existing restrictions on its use. It is important that law enforcement personnel handling this information be trained and knowledgeable on the applicable disclosure rules.[17]

2. Proactive sharing of information between the FIU and investigating authorities

Both the FIU and the investigative authorities should seek to work together as a team, sharing information in appropriate circumstances to support financial investigations. Providing a FIU with an information requirement –detailing information priorities– can assist the FIU in identifying useful information for spontaneous dissemination. Many investigative authorities have seconded personnel working in the FIU, or FIU personnel seconded to investigative authorities in order to facilitate co-operation and information exchange. Single points of contact in investigative authorities and the FIU can also assist consistent, efficient information exchange.

Documenting how competent authorities and FIUs interact and establishing communication channels can provide clarity on the procedures and processes that are required in order to exchange information appropriately. Formal arrangements between investigative authorities and the FIU can be documented in MoUs, memoranda of agreement (MoAs) and standard operating procedures (SOPs). Agreeing on the use of standard electronic reports and request forms that can be securely exchanged between the FIU and investigative authorities can also facilitate efficient exchange of information. When exchanging bulk or structured data in relation to financial investigations (such as computer files with analysis results) consideration should also be given to the compatibility of the software used by competent authorities and the FIU.

Regarding STRs in particular, it should be noted that a financial investigator's understanding is often greatly increased when STRs or disclosure related information is compared with information from other sources (including existing intelligence on illegal activities, criminal records, ongoing investigations, historical investigative reports, and in some cases income tax records). It is therefore essential that law enforcement and the FIU work together to identify those STRs that merit further investigation and ensure that both parties understand what checks have been conducted and which aspects of the disclosure are the most useful to pursue.

The need for efficient utilization of limited resources is a challenge faced by most investigators. When necessary, STRs should be prioritized on the basis of their relative

significance, as well as the general investigative priorities and strategies of the economy. Where a large number of STRs are generated each month, software that works on the basis of pre-established criteria is usually needed to narrow the field of STRs. After such a basic filter, experienced and sufficiently trained support personnel can be designated to continue the prioritization exercise.

3. Use of FIU's intelligence as evidence

Financial disclosures and FIU analysis are usually considered a particular category of information. As stated, they constitute a particularly valuable source of information to law enforcement and, particularly, financial investigators. Given that the main focus is on the use of STRs, the unique nature of this data should be highlighted.

In most member economies, STR information is used for intelligence purposes and is not directly used as evidence in court proceedings. Intelligence information obtained through FIUs shall usually need to be re-obtained through Court proceedings, whether domestically or through mutual legal assistance requests, when the information has been obtained from a foreign FIU. The rationale behind this principle is that the restrictions of individual rights –sometimes privacy, sometimes property- which might follow the introduction of such information into a legal proceeding are subject to Court authorization.

In addition, and for the same reasons, there are also strict confidentially rules associated with access to and use of this information. It is essential that only competent and appropriately trained law enforcement officers have access to this information.

4. Ensuring the proper use of financial intelligence analysis and data

Information sharing and feedback among the FIU, other domestic partners and international counterparts must be subject to strict safeguards –as set out in law or cooperation agreements– to ensure proper use of the data.

It is important to determine how intelligence can be made available to operational authorities and developed into investigative leads or evidence. In order to promote the timely sharing of information, especially at the international level, FIUs can provide guidance on information handling and, where possible, prior consent to its sharing. Such arrangements are usually discussed bilaterally between FIUs in order to address privacy concerns and to ensure that the information is shared lawfully and appropriately with the competent authorities conducting a financial investigation. If prior consent (also

known as third party rule) is required, FIUs should establish mechanisms whereby such consent is obtained in a timely manner.

Because of the practical differences among jurisdictions, there is no exact model for STR utilization that would necessarily fit every member economy. Regardless, member economies should consider putting into place mechanisms that allow their investigative authorities a prompt delivery of FIU information and analysis in furtherance of their investigations. The procedures for delivery should be clearly delineated and subject to strict safeguards to ensure proper security and use of the information. Any model should have in place monitoring systems while ensuring that the process is free of unnecessary hurdles.

C. International cooperation with investigative purposes

International cooperation is highly important for successful investigations and, in particular, for financial investigations. Financial investigations often reach beyond domestic borders and gathering of evidence abroad is a key element in many corruption and money laundering investigations. In complex cases involving many jurisdictions, where information possessed by one of the economies is usually not enough to show an illegal scheme, contacts with law enforcement authorities of other economies involved and the proactive exchange of information are a key factor of success in investigating and prosecuting a case. In investigations ending with asset repatriation, international cooperation will also be fundamental. The combination of informal cooperation among law enforcement authorities and formal international cooperation mechanisms has led to many successful corruption investigations worldwide.

It is thus important that competent authorities from all member economies immediately focus on both formal and informal international cooperation efforts throughout the case, ensuring they can rapidly, constructively and effectively provide the widest range of international co-operation in relation to corruption offences.

International cooperation can be informal or formal. Informal cooperation is usually referred as the mechanisms for obtaining intelligence with investigative purposes; formal channels of international cooperation refer to the procurement of information with evidentiary purposes. Formal mutual legal assistance will always be necessary when the requested assistance either involves coercive measures –e.g., compulsory summoning of witnesses- or the restriction of individual rights –e.g., restraining or confiscation measures-, which will normally require Court authorization.

While formal cooperation is channeled through Mutual Legal Assistance requests or other formal requests to foreign economies through a designated central authority, typical informal channels used by financial investigators include:

- Contact existing liaison officers or investigators in or of the foreign jurisdiction.
- Exchange information between national (or regional) police units using channels such as INTERPOL and other regional law enforcement bodies.
- Inform the national FIU, which has a possibility to contact its foreign counterparts and collect further intelligence through the Egmont Secure Web or by other means.

The remainder of this section describes the main channels for informal international cooperation as well as the most salient requisites of mutual legal assistance requests.

1. Informal cooperation networks

The establishment of informal contact between officers and investigators of member economies should be the first step towards effective cooperation. Whenever possible, information or intelligence should initially be sought through police-to-police contact, which is faster, cheaper and more flexible than the formal route of mutual legal assistance. Such contact can be carried out through local liaison officers, under any applicable memoranda of understanding, through Interpol, or through any regional arrangements that are available.

Through such informal assistance investigators can gather information more quickly, build the necessary substantive foundation for an eventual formal request, and develop a strategy that best accords with the advantages and limitations of the legal systems of the involved jurisdictions. Both the United Nations Convention against Corruption (UNCAC)[18] and the FATF Recommendations[19] highlight the importance of the availability of informal cooperation and assistance mechanisms among counterpart agencies.

Economies should ensure that domestic laws authorize direct contact between domestic authorities—including law enforcement agencies, financial intelligence units, and prosecutorial agencies—and their foreign counterparts. Authorities in requested jurisdictions should be permitted to provide some information and informal assistance to their foreign counterparts without requiring a formal MLA request.

Most member economies are in the position to provide the following types of informal assistance without a written formal request:

- public records, such as land registry documents, company documents, information about directors and shareholders, and filed company accounts;
- potential witnesses to determine if he/she is willing to cooperate voluntarily and take statements from voluntary witnesses, provided that contact with witnesses is permitted under such circumstances;
- provide basic subscriber details from communication and service providers that do not require a court order.[20]

Table 4: Best practices

Best practices to help strengthen legal frameworks and ensure that asset tracing and financial investigations can be conducted effectively include having appropriate procedures and the legal framework to allow the informal exchange of information, the use of appropriate regional and international bodies to facilitate cooperation, the spontaneous sharing of information with proper safeguards and the entering into asset sharing agreements.[21]

➢ Police-to-police communication

Police-to-police communication can be a very useful way for the APEC economies to acquire information, especially in the early phases of an investigation that may later on require a formal MLA request.[22] Matters such as locating witnesses or suspects, conducting interviews, sharing police files or documentation on a person or assessing whether a witness would be prepared to speak with investigators can all be done through police agencies, with no need to resort to a mutual legal assistance request. Police agencies have well-established networks of *liaison* officers throughout the world, and lines of communication and protocols with the police agencies that they consistently deal with. INTERPOL is the most developed worldwide police network.[23]

➢ Agency-to-agency communication

An example of agency-to-agency communication is the one between the central authorities, investigatory authorities as well as the liaisons that report to them. These lines of communication complement the lines that the police and INTERPOL have already established.

- Consular communications

Some APEC economies rely on their consulates abroad to assist in obtaining information in financial investigations and as a conduct for obtaining help to prepare a formal MLA request. Mexico, for instance, uses its consulates to obtain evidence, declarations or information regarding particular investigations or judicial cases.[24]

a. Personal networking

Personal contacts between members of competent authorities, prosecutors and investigators from the requesting and requested economies (through a telephone call, an e-mail, a videoconference or a face-to-face meeting) and developing working level cooperation are of great importance in order to achieve open communication channels and develop the familiarity and trust necessary to achieve the best results in mutual legal assistance casework.

Relevant information may be obtained more quickly and with fewer formalities through direct contact with counterpart law enforcement agencies and FIUs or from law enforcement attachés. Such contact can be initiated through existing police attaché networks, or between prosecutors' staff of central authorities, through the United Nations International Drug Control Programme (UNDCP) list of competent authorities, or through less formal structures such as the International Association of Prosecutors or simply personal bonds. This kind of assistance may lead to a more rapid identification of evidence and assets, confirm the assistance needed and even more importantly provide the proper foundation for a formal MLA request.

Establishing early contact with foreign counterparts aids investigators in understanding and foreseeing how to address the potential challenges that might emerge from a different legal system, in obtaining additional leads and in forming a common strategy. It also gives the foreign jurisdiction the opportunity to prepare for its role in providing cooperation.

In order to constructively and effectively provide the widest range of international cooperation, it is essential for financial investigators to discuss issues and strategy with foreign counterparts. Such discussions should involve consideration of conducting a joint investigation[25] or providing information to the foreign authorities so that they can conduct their own investigation.

If the financial investigation is in an early stage or if concerns about the integrity or independence of potential counterparts are at stake, discussion from a "hypothetical" perspective is recommended. Such discussions allow all involved parties to get a better understanding of the parameters and requirements of an investigation without having to discuss too many specific details, which can be shared at a later stage if necessary.

Finally, it is important for investigators and prosecutors who deal with corruption cases daily to regularly attend training events and seminars at the regional or international level.

b. The International Criminal Police Organization (Interpol)

Interpol is the world's largest international police organization, with 190 members.[26] It was created in 1923 to facilitate cross-border police co-operation, and support and assistance to all organizations, authorities and services whose mission is to prevent or combat international crime (even where diplomatic relations do not exist between particular jurisdictions). Its four core functions are: (i) to maintain a secure global police communication service; (ii) to provide police with operational data services and databases; (iii) to offer operational police support services; (iv) training and development[27].

c. The Egmont Group

Informal contact with the FIU of another member economy for information purposes can be achieved through direct contact between the implicated agencies or through the Egmont Group, when both members belong to such forum.[28]

The Egmont Group, created in 1995, provides a forum for FIUs around the world to enhance support to their respective governments in the fight against money laundering, terrorist financing and other financial crimes. This support includes:

- expanding and systematizing international cooperation in the reciprocal exchange of financial intelligence information,
- increasing the effectiveness of FIUs by offering training and personnel exchanges to improve the expertise and capabilities of personnel employed by FIUs,
- fostering better and secure communication among FIUs through the application of technology, presently via the Egmont Secure Web (ESW), and
- promoting the establishment of FIUs in those jurisdictions without a national anti-money laundering/terrorist financing program in place, or in areas with a program in the beginning stages of development.

The Egmont Group has now over 130 members.[29]

A secure encrypted capability designed to share information over the Internet; Egmont's Secure Web facilitates communication among group members via a secure e-mail, also allowing them to access meeting minutes and related documents, as well as a variety of published materials of the Egmont Group.

2. Formal cooperation

Formal cooperation is often the only way in which evidence can be obtained from another jurisdiction to be presented in the court. Formal types of assistance include: letters rogatory, letters of request, Mutual Legal Assistance requests and requests under bilateral or multilateral treaties. In order to legally obtain evidence that is admissible in court, investigators and/or prosecuting authorities must make use of the applicable international arrangements which may be based on reciprocity, MoUs, bilateral or multilateral agreements. Once a decision has been made as to which jurisdictions have responsibility for prosecuting and/or investigating different sides of a given case, mechanisms should be agreed in order to ensure that all relevant evidence can be made available in the competent jurisdiction in a form that will allow production in a criminal court respecting the due process of law.

Table 5: The Asia/Pacific Group on Money Laundering (APG)

The Asia/Pacific Group on Money Laundering (APG) is an autonomous and collaborative international organization founded in 1997 in Bangkok, Thailand. It consists of 41 members and a number of international and regional observers. Some of the key international organizations that participate with, and support the efforts of the APG in the region include the Financial Action Task Force, the International Monetary Fund, the World Bank, the OECD, the United Nations Office on Drugs and Crime, the Asian Development Bank and the Egmont Group of Financial Intelligence Units.

The purpose of the APG is to ensure the adoption, implementation and enforcement of internationally accepted anti-money laundering and counter-terrorist financing standards as set out in the FATF Forty Recommendations and FATF Eight Special Recommendations.

The effort includes assisting economies of the region in enacting laws to deal with the proceeds of crime, mutual legal assistance, confiscation, forfeiture and extradition; providing guidance in setting up systems for reporting and investigating suspicious transactions, and helping in the establishment of financial intelligence units.

CHAPTER III. THE GATHERING OF INFORMATION AND EVIDENCE

Prosecuting and proving a crime is often much more difficult than investigating and solving it. Due to the dire consequences of a criminal conviction for the fundamental rights of the convicted person, criminal cases have a stricter burden of proof than civil cases. In order to overcome the presumption of innocence and for a person to be convicted, that person must be proved guilty, either with certainty or –depending on the economy's legal system- "beyond any reasonable doubt".

Therefore, the gathering of credible information and evidence that supports the commission of a crime is often essential in the early stage of an investigation, since it allows law enforcement agencies to move forward by securing warrants for search, seizure, or intercepting phone calls and e-mails.

In order to be Court admissible, evidence must be obtained in accordance with the applicable criminal procedure laws as well as the constitutional rights of the defendants or any other affected third party. Due to the fact that unlawfully obtained evidence could be declared inadmissible in court and therefore jeopardize the success of the prosecution or confiscation, all evidence should be legally obtained and, to that purpose, law enforcement agencies should be well aware of the legal framework applicable to the evidence collection process. Legal experts' advice should always be sought by agencies in dealing with the gathering of evidence.

Once evidence has been legally collected, it should be subject to an assessment in order to review the progress of the investigation and explore whether any additional line of inquiry can be identified.[30] Investigators are advised to follow a standard model of evaluation –like the one shown in the following flow figure– since it will allow them to evaluate the collected material in a consistent, structured, and auditable way.[31]

1 Setting the objective of the evaluation

In the early stages of an investigation, the objectives are likely to be broad and concerned with whether a crime has been committed, whether a suspect and witnesses can be identified, what material can be gathered, etc.

As the investigation progresses and initial ends are achieved, the objectives will narrow. They will vary depending on the crime, the available material and the stage of the investigation. The evaluation process should be sufficiently flexible to accommodate such changes.

2 Evidential filters

Relevance

Whether gathered materials have some bearing on any offence or person under investigation, or on the surrounding circumstances of the case, must be evaluated

Reliability

The reliability of materials should be reviewed during the evaluation process to ensure that any potential problems have not been overlooked. Investigators should have a clear understanding of the impact the reliability of material may have on the investigation and the strength of the prosecution case. An element can have high reliability if it can be corroborated by an independent source, and less reliability if it cannot be corroborated and conflicts itself with other materials gathered in the investigation.

Admissibility

This test should ensure the investigators that the gathered materials will be available to the courts in an evidentially acceptable format. Investigators must be aware of the legal framework and must seek legal advice on what constitutes an acceptable evidential format in relation to any material.

3 Organizing knowledge

In the first instance the objective of an investigation is likely to be broad and concerned with establishing what information there is, what type of incident is being investigated, whether or not a crime has been committed and if there is a suspect. The 5WH formula (Who – What – When – Where – Why – How) has been found to be a highly effective way for investigators to organize their knowledge in the early stages of an investigation (See Chapter IV, Section B.3 for further development of this formula regarding profiling).

Who are the victim(s), witnesses, and suspect(s)?
Where did the offence take place?
What has occurred?
When did the offence and other significant events take place?
Why was this offence committed?
How was the offence committed? Assess the use of skills or knowledge used by the offender.

Subsequent evaluations will replace the broad objectives with more specific objectives. The way in which investigators then choose to organize their knowledge will change to match these more specific objectives.

4 Testing Interpretation

There are a number of ways in which investigators can test the validity of their interpretations of the gathered material.

Self-review: Investigators should thoroughly check their work and review any assumptions they have made during the evaluation process.
Peer review: Checks by supervisors or colleagues provide a second opinion on the interpretation of material.
Expert review: Where investigators use material produced by experts such as forensic scientists, they should consult the expert to ensure that the outcome of the evaluation is consistent.

Formal review: In complex cases a formal review of the investigation can be carried out by a suitably qualified officer.

Table 6: Best Practices - Evidence gathering.

SOURCE: KOH TECK HIN, Investigation and Prosecution of Corruption Offences, (Singapore), Resource Material No. 86, Visiting Experts' Papers, 14th UNAFEI UNCAC Training Program, Tokyo, March 2012, pp. 104 ff.; CORRUPT PRACTICES INVESTIGATION BUREAU (CPIB), elaboration dated Dec 2013.

When we make use of the four competencies of intelligence, interview, forensics and field operations, we also focus on collecting and consolidating the evidence. From the evidence, we review the case. Sometimes, we sit together and discuss in case conferences to go through these issues - Do we have the evidence to charge anyone? What evidence is there when we proceed to charge? We make use of an evidence matrix (see table attached below).

OPS "X"
Evidence Analysis Framework (For Corruption Offences)

Evidence of Accepting/Obtaining/receiving		Evidence of Giving/Offering/Promising	
Admitted by:	Nature of Admission	Admitted by:	Nature of Admission
Implicated by:	Nature of Implication	Implicated by:	Nature of Implication
Documentary Evidence:	Nature of Documentary Evidence	Documentary Evidence:	Nature of Documentary Evidence
Other Evidence:	Nature of Evidence	Other Evidence:	Nature of Evidence
Evidence of Corrupt Intent			
Giver		Receiver	

Evidence Analysis Framework (For Other Offences)

Ingredients of the Offence 1)	
Admission by accused:	Nature of Admission
Witnesses' evidence:	Nature of evidence
Documentary evidence:	Nature of Documentary Evidence
Ingredients of the Offence 2)	
Admission by accused:	Nature of Admission
Witnesses' evidence:	Nature of evidence
Nature of evidence	Nature of Documentary Evidence

Follow-up Actions

Subject/ Witnesses	Gaps identified	Follow-up actions	Action by	By when	Status Report

This matrix has facilitated our case review and decision making process. Evidence of accepting/receiving/ obtaining gratifications is reflected in the table, where officers document *actus reas*, inputting details of the corrupt transactions which the subject has admitted to in his statements, e.g. when did the transaction occur, who did he hand the gratification over to, what is the documentary evidence, etc. Next to the information is the detailing of documentary or other evidence of giving/offering/promising of the corrupt transactions. Usually, for easier reference, the evidence for giver and receiver involved in the same transaction are placed next to each other, quoting the exact paragraph of the subject's statements where the information was extracted from. As for the evidence on corrupt intent, it is also recorded in the table, and it includes details such as what the gratifications are meant for.

In addition, we also need to address the legal aspects. We understand that in some economies, the anti-corruption agency has their in-house legal experts and some agencies also conduct prosecution themselves In the Singapore system, the Corrupt Practices Investigation Bureau (CPIB) does not have in-house legal experts but is part of the criminal justice system which comprises the Attorney-General's Chambers (AGC), the Courts and other law enforcement agencies. The Courts represent the adjudicating arm; the AGC serves as the prosecuting arm, while CPIB and other law enforcement agencies form the investigative arm. CPIB is the only agency authorized to investigate into corruption offences. For all corruption cases, when investigation is concluded, the Public Prosecutor's consent must be obtained before prosecution against the corrupt offender can proceed. Thereafter, the accused will be brought before the court which will determine if the offender is guilty of the offence(s). In sum, after CPIB completes our investigation, we will submit our findings (including recommendations of corresponding charges to the AGC) for their consideration. AGC's decision on whether to proceed with prosecution is final. There is thus an inherent check and balance mechanism in our criminal justice system where the powers to investigate and prosecute corruption offences are separate and do not reside with any one agency.

In terms of prosecution, as we are prepared to prosecute both the givers and receivers of bribes, we have to stage our prosecution of the accused persons in sequential order. Sometimes the receiver is prosecuted first and the giver is the prosecution witness. After the case is over, the giver is prosecuted and the receiver in turn becomes the witness. This can present some challenge especially when there is not much independent evidence apart from what the giver and receiver say about the crime. Therefore, as we adopt this tough stance against both sides of the corruption crime, it is the responsibility of CPIB to ensure that it gathers strong evidence on the case so as to be able to prosecute all parties involved. So far, our conviction rate is of above 95% each year and this bears testimony to the strength of cases brought to the Court.

There are instances where the only evidence we have is from the giver and the giver is not willing to testify unless he is given immunity from prosecution. As a rule, the Attorney General's Chambers does not grant immunity easily. If immunity is granted, it will be under exceptional grounds.

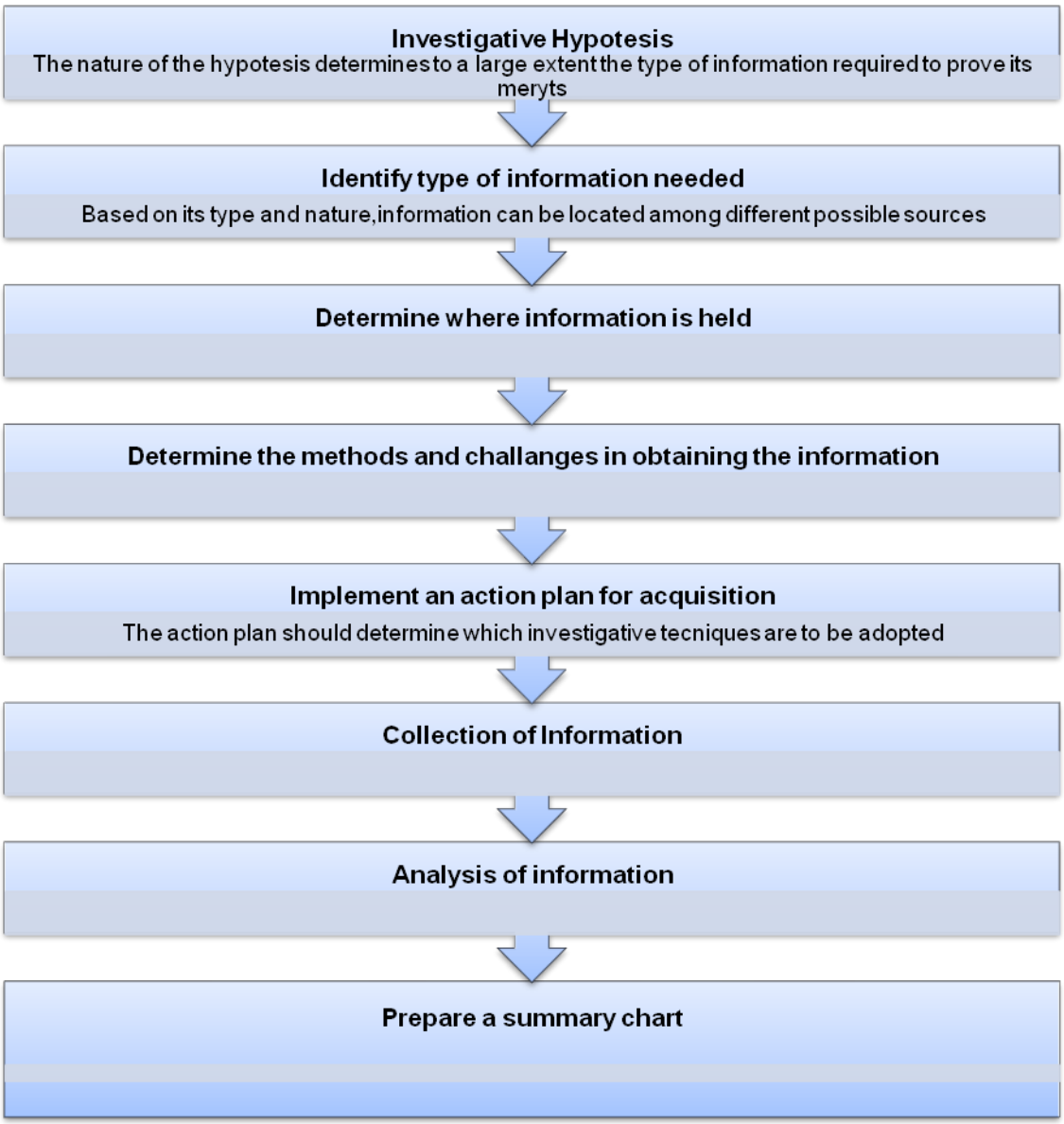
There may be cases in the public sector where after an investigation there is no evidence of corruption but there is evidence that the public official had infringed some government rule or regulation. In such situations, CPIB will provide the information to the Public Service Commission or to the officer's Department or Ministry for them to take departmental disciplinary proceedings against said officer.

In some cases, besides dealing with the culprits, after the case is over, CPIB may identify flaws or loopholes in the system, work processes or procedures of the affected government departments and offer some recommendations or suggestions for them to consider as they work towards mending the flaws and loopholes.

A. Sources of information

A variety of sources can be relevant to financial investigations, including interviews, searches, forensic examination of computer(s), collection and analysis of financial and business records, tax authorities' reports, etc.[32]

The process illustrated in the following flow chart synthesizes a recognized international best practice to be followed all along the process of gathering of information and evidence.



There will be differences within each economy in the way that various types of information can be made available to investigative authorities and this may be influenced by legal requirements. The producers and owners of the relevant pieces of information and intelligence products will also differ between economies[33].

There are several ways to categorize potential data sources. The Inter American Drug Abuse Control Commission of the OAS (CICAD) has proposed a classification of sources of information that is also applicable to corruption investigations:[34]

Patrimonial
Sources of information related to asset ownership of an individual or company (vehicles, real estate, horses, jewels, industrial real estate, airplanes, stocks, weapons, etc.)

Personal
Sources of information related to data of an individual such as marriage status, contact information, phone number, passport number, occupation, etc.

Legal
Sources of information related to civil, criminal, business, and labor litigation of an individual or company.

Business
Sources of information related to economic activity or business conducted by an individual or company.

Police
Sources of information related to traffic infractions, fines, or any other relevant police information.

Corporate
Sources of information related to incorporation of companies and changes in partnership quota, trust funds, board of directors, etc.

Normative
Sources of information related to an economy's norms and regulations, and its jurisprudence.

Another useful way to categorize information is according to the nature of the source where it can be retrieved:

Criminal records and intelligence

Law enforcement information related to the subjects under investigation. Information such as previous arrests, indictments, convictions, but also reports of links with known criminals. Criminal information is typically gathered from surveillance, informants, interviews/interrogation and data research, or may be just picked up "on the street" by individual police officers.

Local Force Intelligence System

Information, including bank account details and telephone numbers, may be held on local databases.

AML/CFT Disclosures

In addition to suspicious transaction reports (STRs), this includes other information as required by national legislation such as cash transaction reports, wire transfer reports and other threshold- based declarations or disclosures.

Financial Information

Information about the financial affairs of entities of interest that helps to understand their nature, resources, structure and capabilities, and it also helps predict future activity and locate assets. This goes beyond the information contained in AML/CFT disclosures and is normally maintained by private parties, including bank accounts, financial accounts, other records of personal or business financial transactions and information collected in the context of meeting customer due diligence (CDD) obligations.

Examples:[35]

Financial Institutions

Information held by financial institutions can show the lifestyle of a person and whether they are living beyond their means. These can inform an investigator of payments to and from other persons, the lifestyle of the individual (their wealth, the turnover in their account), their spending patterns (for example, where they went on holiday, their travel, meals, hobbies and other interests), and any financial problems.

Commercial Service Providers

Merchant service providers, such as mobile phone companies, utility companies or firms that deal with merchants' claims for reimbursement for credit or debit card payments by customers, hold a variety of information of potential use to an investigation. This can include a person's location at a certain time or details of any electronic payments. Investigators can apply for production orders to obtain information from the financial institution that administers the chip and PIN or swipe systems (such as Link), which can then be followed up.

Credit reference databases

Credit reference agencies provide data access systems that can be used in criminal investigations allowing authorized officers to obtain information on an individual's financial relationships and status. This information can assist in the prevention or

detection of crime and apprehension and prosecution of offenders, or the assessment or collection of any tax or duty.

Classified information
Information that is gathered and maintained for national security purposes to include terrorism financing information. Access is typically restricted by law or regulation to particular groups of persons.

Open Sources
All information that is available through open sources such as the internet, social media, print and electronic media, as well as via registries operated publicly or privately.

Regulatory information
Information that is maintained by regulatory agencies; access is typically restricted to official use only. This category of information could be held by central banks, tax authorities, other revenue collecting agencies, registry agencies, etc.

Table 7: Warning – Do not leave footprints

SOURCE: Association of Chief Police Officers **(**ACPO), *Practice Advice On Financial Investigation,* 2006, p. 20.

There are various open and closed sources where financial information can be obtained. The enquiries made to obtain this information can, however, leave their own footprints. If an FI makes an enquiry with a Money Laundering Reporting Officer (MLRO) at a financial institution, the institution will make a note of the enquiry, including its purpose. The investigation being conducted may involve the use of covert investigation techniques. As such financial enquiries could result in those investigations being compromised. Prior to making the relevant financial enquiry, consideration must be given to the type of investigation being undertaken. As such any enquiries should be progressed in consultation with the FIU.

B. Gathering peripheral evidence

At the preliminary stage of any investigation, law enforcement agencies should rapidly gather information from all available sources. Data collected in this phase can therefore provide the factual basis to bring the investigation to the next stage, which might involve the need for a judicial warrant to be applied for before the competent authority.

Because the data collected might be filed in a judicial proceeding, the acquisition process is a sensitive moment.

At this stage, immediately available sources are in particular the so-called “open sources” and government agencies databases (publicly and not-publicly available). Those are typically referred to as the source of first resort, because every information collector should exploit them as the first step in the information-collection process.

1. Open Sources

a. General Aspects

Open source information has been defined as «publicly available information that anyone can lawfully obtain by request, purchase, or observation».[36] The use of open sources techniques is a rising area of intelligence gathering. As the public globally embraced the World Wide Web in the mid-to-late 1990s, the internet emerged as the primary source for search for all types of information. In the so-called “information age”, the Internet provides access to a huge amount of significant, updated information, which has proven to be of dramatic importance for law enforcement agencies. In other words, almost everything is online: in 2008, for example, Google had indexed 1 trillion of addresses, which constitutes just a small part of the Internet.[37]

Originally developed for security purposes, the internet became widely used for academic and commercial research in the 1980s. In the late ‘90s, the U.S. GAO had already noted that investigators would have found significant advantages on accessing sources online rather than using any other information medium, and that «the internet provides enormous resource potential for investigators in a timely and cost effective manner and is often more up-to-date than its paper counterparts.»[38]

Internet-based services using Web 2.0 technology have become increasingly popular. Web 2.0 technologies are a second generation of the World Wide Web as an enabling platform for web-based communities of interest, collaboration, and interactive services. These technologies include web logs (known as “blogs”), “wikis,” which allow individual users to directly collaborate on the content of Web pages; “podcasting,” which allows users to publish and download audio content; and “mashups,” which are web sites that combine content from multiple sources. Web 2.0 technologies also include social media services, which allow individuals or groups of individuals to create, organize, edit, comment on, and share content. These include social networking sites (such as Facebook and Twitter) and video-sharing web sites (such as YouTube).[39]

As reported by the U.S. Government Accountability Office in 2011, social media-related sites have become the most visited websites in the web.[40] Of course, quantity of information does not equal quality of information. Investigators must ensure that the information collected from open sources is accurate and reliable. The challenge, particularly when massive amounts of information are available, is to make good end-user decisions about what information should be kept and which information should be discarded.[41]

Open source information has often held a second-class status in the intelligence world because of the erroneous assumption that people, movements, and conditions that pose threats would not have information available about their intent, characteristics, or behavior in the open.[42] However, information can be made publicly available for many reasons: because the person needs so or the applicable laws require so, due to the individual's carelessness, and so on.

Open sources can be used for a variety of purposes. One of the most common uses is to identify and verify a wide range of facts: personal identity information, addresses and phone numbers, e-mail addresses, vehicles known to have been used, property records, are among a wide variety of other facts that can easily be identified through open source public and commercial databases and directories.[43] This type of tool can also be used as a mean to identify criminal offenders. Indeed, it has been remarked that in a surprising number of cases people made incriminating statements in open sources. While those statements alone will not meet the burden of proof for conviction, they clearly establish a criminal predicate and basis for further inquiry.[44] Finally, open sources can help in understanding the motivation or rationale of individuals involved in criminal behavior.

Today, the significance of open sources techniques has been widely recognized, and they have proven to be especially useful in corruption and money laundering investigation, as well as in the process of recovering stolen assets.[45] Its importance has also been remarked by the US 9/11Commission, which recommended to add a new Open Source Agency to the U.S. intelligence structure.[46] For these reasons, law enforcement agencies should rely upon open sources techniques more often, which should be incorporated in the agencies' intelligence plan.

Open sources intelligence includes methods of finding, selecting and acquiring from publicly available sources, and analyzing such information to produce credible intelligence. Open source is distinguished from research in that it applies the process of

intelligence to turning hard data and information into intelligence to support strategic and operational decisions.[47]

Open source information is wide-ranging. Examples of categories of open source information include:[48]

All types of media
Example: www.newslink.org
Shortwave broadcasts and conversations
Examples: www.shortwave.be, www.blackcatsystems.com/radio/shortwave.html.
Publicly available databases
Examples: www.searchsystems.net, www.factfind.com/database.htm
Social networking sites and web-based communities
Examples: www.facebook.com, www.twitter.com, www.myspace.com
Directories
Example: www.mypeoplesearch.com (only US and Canada users allowed)
Databases of people, places, and events
Examples: www.namebase.org, www.searchsystems.net, www.blackbookonline.info
Open discussions, whether in forums, classes, presentations, online discussions on blogs, or general conversations
Wikis
Example: www.wikipedia.com
Government reports and documents
Scientific research and reports
Example: www.fas.org

Statistical databases
Example: www.bjs.gov

Commercial vendors of information
Example: www.acculeads.com

Web sites that are open to the general public even if there is an access fee or a registration requirement

Search engines of Internet site contents
Examples: www.google.com, www.itools.com, www.aks.com, www.yahoo.com,

Open source intelligence requires a certain degree of specialization. As remarked by experts, the effective use of the internet to gather information is a specialized area of work, and secure methods of searching must be employed so as not to compromise operations.[49]

Intelligence in this sector requires different skills, such as the ability to analyze aggregate information. As it has been pointed out, "the information obtained from open sources tends to fall into two categories, namely one involving information about individuals, and, secondly, involving aggregate information. The aggregate information available is extensive which is where the skills of a qualified analyst come into play as it is a real challenge to assess what is reliable and what is relevant for the purposes of constructing intelligence. Consider some of the new databases, often commercially available, which are able to provide enormous detailed analysis of current trends, companies and individuals. It is no surprise therefore that law enforcement agencies are now increasingly using these methods".[50]

- **Legal issues**

From a law enforcement perspective, one of the values of open source information is that it can be usually searched for and collected without a legal process. However, it raises important legal issues, i.e. civil rights issues related to the retention of open source information for the intelligence process.

Agencies must be vigilant in the managing of open source information because of the regulatory framework that might apply to information retention in a criminal intelligence records system. Indeed, when information is being gathered via open source and is being retained as intelligence, human and constitutional rights claims may arise.

Open source can lead to the mining of important and sensitive information about an individual, for example, a person's credit rating. Therefore, once the information is retained and forms part of an intelligence assessment and a file, questions and processes need to be carefully considered to ensure compliance with the broader issues under human and constitutional rights.[51]

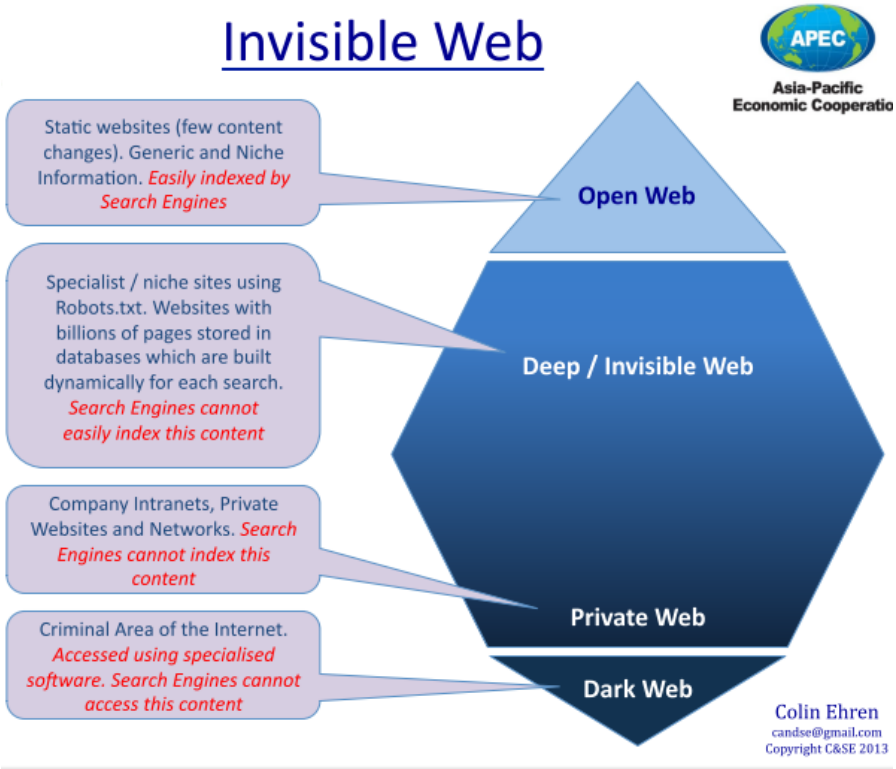
The key is not the source of the information but what is being retained and how it is being retained. On a general basis, it is possible to operate a distinction among raw information obtained from open sources into two categories, where only the first one can raise civil rights issues and therefore requires to be specifically addressed:[52]

Information about individuals and organizations
As a general rule, when a law enforcement agency conducts an open source search for information, the agency should assume that civil rights protections attach to any information that identifies individuals or organizations, no matter how innocuous that individual piece of information appears to be.

Aggregate non identifying information
As a general rule, usually no civil rights attach to aggregate information or descriptions of issues, trends, ideologies, and so forth that does not identify an individual or organization.

b. Search Engines and the Deep, or Invisible Web

Currently, hundreds of search engines are available to retrieve information from the internet. However they can easily index only the "Open web", i.e. static websites, with generic and niche information. This is just the tip of the iceberg that represents the information present on the internet.



Picture taken from: EHREN, Colin, "Challenges of Gathering Evidence from the Internet", presented at the APEC Anti-Corruption and Transparency Working Group (ACTWG), *Capacity Building Workshops on Designing Best Models on Prosecuting Corruption and Money Laundering Cases Using Financial Flow Tracking Techniques and Investigative Intelligence for Effective Conviction and Asset Recovery to Promote Regional Economic Integration*, Santiago, Chile, 11-13 June 2013.

There exists another part of the web, usually referred to as the "deep" or "invisible" web. Deep web is the vast repository of information, that search engines and directories do not have direct access to. It is described as the specialist/niche sites using robots.txt, websites with billions of pages stored in databases, which are built dynamically for each search. Information in databases is generally inaccessible to the software spiders and crawlers that create search engine indexes.

This part of the web can visually be represented by the underwater part of an iceberg, and constitutes the major part of the information stored on the web. Common estimates suggest that the deep web contains 500 times the content that is found in the visible web.

In July 2001 it was found that:[53]

- deep web is 400 to 550 times larger than the World Wide Web;
- 7,500 terabytes of information compared to 19 terabytes on WWW.
- 550 billion documents compared to 30 billion on the WWW.
- 200,000+ deep Web sites.

- 60 of the largest sites collectively contained over 40x the information on the WWW.

The deepest part of the iceberg represents “Private Web”, i.e. company intranets, private websites and networks, and the “Dark web”, the criminal area of the web, which is only accessible through specialized software. Neither of the two can be indexed and accessed by search engines.

Five broad types of content constitute the invisible web:[54]

The content of web-based databases
Information stored in databases is accessible only by query to the database and is not picked up by the web crawlers used by search engines. This is distinct from static, fixed web pages, which contain documents that can be accessed directly. A significant amount of valuable information on the web can be generated from databases.

Non-textual files
These include multimedia files, graphics files, software, and documents in formats such as Portable Document Format (PDF). Web crawling has a limitation in searching the content of these types of files. Web crawlers can identify file names and extensions (e.g., .jpg, .wmv, .pdf, etc.) of such files, but cannot identify the content of these files during the web crawling process. Essentially, these files are not in HTML 90 format, therefore a great deal of information and data is not picked up from these files by traditional searches.

Script-based web pages
These are web pages that are written in script coding, other than HTML and/or those with URLs 91 that contain a “?”.

Content available on sites protected by passwords or other restrictions
The content of web sites protected by some degree of access through rigorous password protection or a Virtual Private Network (VPN) will not be identified by search engines. There is a continuum of identifiable and non-identifiable information from these types of web sites depending on what types of information the site owners elect to be publicly accessible (often for marketing purposes) as well as the degree of security applied to the site (in some instances the web site’s security is limited and some data can be identified). A significant amount of information from these sites is not identifiable through traditional search engines.

Pages deliberately excluded by their owners
A web page creator who does not want his or her page captured in search engines can insert special meta tags that will cause most search engines' crawlers to avoid it.

Search Engines cannot easily index this content, but that doesn't mean that deep web is not searchable. Investigators must rely on tools that can locate valuable open source deep web information.

The most effective ways to search the deep web is to use search utilities that are designed to explore specific databases. While this still reaches only a portion of the deep web, the information gained from these databases can be extremely valuable. Deep web searching of databases typically requires accessing a variety of web sites to search for the desired information.

What should be apparent is that much of the deep web is not hidden in a surreptitious manner. Rather, it is hidden because it contains information in formats or architectures that are not readily identifiable by standard search engine technologies. As a result, it takes specially designed search utilities and greater effort by the user to identify and capture deep web information.[55]

It should be noted that Internet service providers and companies that operate social networking web sites typically have a published policy and guidance to work specifically with law enforcement agencies.[56] However, when the process goes beyond information that is openly available on the Internet, it is technically not open source information. This issue will therefore be addressed in Section IV. B. 4.

c. Social Media

Social media is a category of the internet-based resources that allows users to generate their own content and then share that content through various connections.[57] It is, at its core, a tool for communication that focuses on integration, collaboration, and interaction, and that has become an integral part of daily life for people of all ages. Social media accounts for 22% of time spent on the internet.[58]

The use of social media in policing is an issue that has only begun to emerge in the last few years. In a recent survey of 800 law enforcement agencies in the United States, 88 percent of agencies reported using social media.[59] According to a July 2012 survey by LexisNexis Risk Solutions, of 1,221 U.S. federal, state, and local law enforcement agencies that use social media in some way, four out of five agencies said they use social media for investigations.[60] The top use is for crime investigations, followed by crime anticipation. Agencies may use social media as an investigative tool when seeking evidence or information about a wide range of criminal activities.[61]

Social networking sites provide a multitude of information about individuals and persons with whom they interact. Social media sites contain identity information of the user and his or her contacts, often with photographs, as well as private messages and statements about beliefs and behavior. While some information, such as a private message, is subject to legal process, a great deal of information is available as an open source.[62]

Examples of social media include blogs, social networking sites, microblogging sites, photo- and video-sharing sites, location-based networks, wikis, mashups, RSS feeds, and podcasts.[63]

- **Facebook** (www.facebook.com)

Social networking site launched in 2005 that lets users create personal profiles describing themselves and then locate and connect with friends, co-workers, and others who share similar interests or who have common backgrounds. Individual profiles may contain—at the user's discretion— detailed personal information, including birth date, home address, telephone number, employment history, educational background, and religious beliefs[64]. Users can also instantly share their exact geographical location by using the "check-in" option. Facebook claimed to have 1.49 billion monthly active users worldwide at the end of June 2015.[65]

- **Twitter** (www.twitter.com)

Social networking site that allows users to share and receive information through short messages that are also known as "tweets." These messages are no longer than 140 characters in length. Twitter users can establish accounts by providing a limited amount of PII but may elect to provide additional personal information if they wish. Users can post messages to their profile pages and reply to other Twitter users' tweets.[66] Users can "follow" other users as well—i.e., subscribe to their tweets. In June 2015, Twitter reported facilitating the delivery of 500 million tweets every day.[67]

- **YouTube** (www.youtube.com)

Online video community that allows users to discover, watch, upload, comment on, and share originally created videos. Similar to Twitter, users can establish accounts on YouTube with only limited amounts of personal information, although they may choose to provide more detailed information on their profile page. Users can comment on videos posted on a page either in written responses or by uploading their own videos.

According to YouTube, during 2010 more than 13 million hours of video were uploaded.[68]

- **Other commonly used social media**

LinkedIn: www.linkedin.it
Google Groups: groups.google.com
Yahoo Groups: groups.yahoo.com
Windows Live Messenger: messenger.live.com
Skype: www.skype.com
Yahoo Messenger: messenger.yahoo.com
MySpace: www.myspace.com
Orkut: www.orkut.com
Internet Relay Chat
Usenet Talk Groups
Dedicated Discussion Forums
Dating sites (Muslim Match, Uniform Match, Adult Friend, etc.)
Reunion Sites

i. Social Media Monitoring Tools

Law enforcement agencies can rely on social media monitoring tools to capture data and monitor social media sites. These tools offer the ability to search for keywords and thus enable law enforcement to aggregate large amounts of data and refine them into smaller items of interest.[69] For example:

Twitterfall
Netbase
Trackur
CrowdControlHQ
Socialpointer

ii. Compromise Issues & Internet Footprints

There exist multiple ways to access the internet, nonetheless it is recommendable that all detailed or sensitive internet research or open source investigations should be undertaken on a covert or unattributed and registered PC, using a covert or unattributed internet connection. That's because the agency internet footprint could compromise an investigation or an intelligence operation.[70]

If both a covert and a not-covert user search for the same target, the covert user may then be linked to the not-covert user and therefore recognized as an investigator.

Web pages can include images or adverts from third parties, which can leave cookies on your PC. Companies such as "Ad-Image.com" are able to compile a significant profile on you and your surfing habits, which are traded or sold to partners or customers.

iii. Storage of data and gathering of evidence

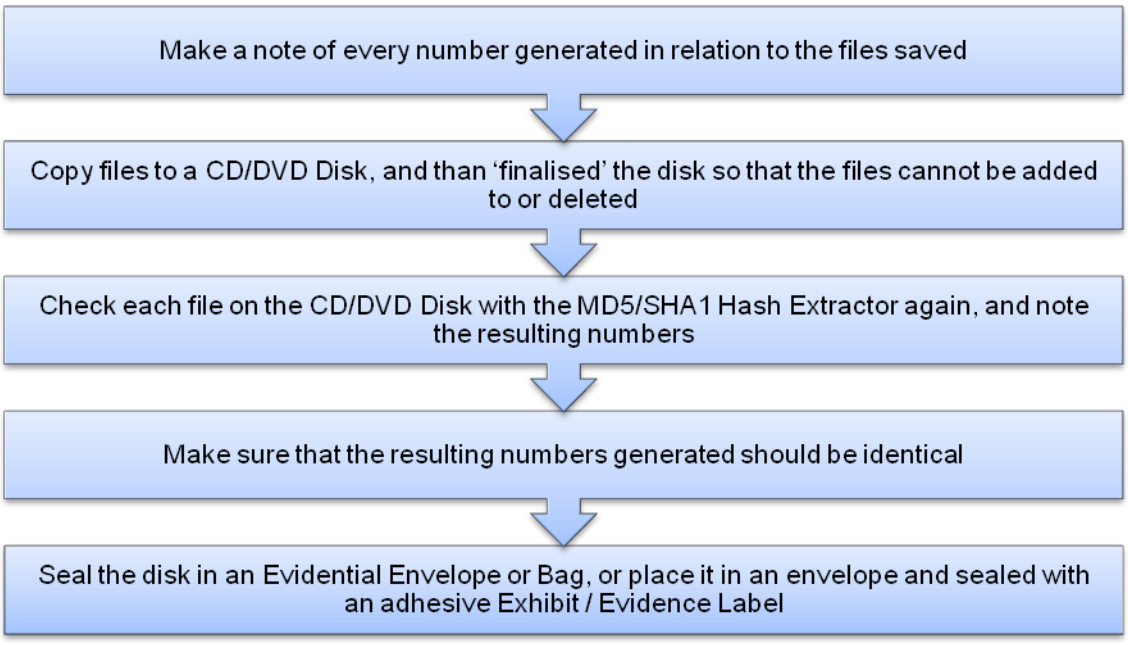
To ensure that a social media investigation can produce high-quality, actionable intelligence, agencies must consider a number of issues, including which types of online content should be viewed and who will conduct the observation and analysis.[71]

Agencies might have to deal with a huge amount of data, and should count on social media extraction and visualization tools.

Many different laws may govern law enforcement agency records. Agency policy should cover the documentation, storage, and retention of social media information gathered for criminal investigations. Information gathered from social media sites should be printed and electronically archived.[72]

When saving and moving data the investigators must ensure that the evidential chain is preserved, in order to use the information as a proof.

In order to preserve the evidential chain, experts recommend making use of an MD5 or SHA1 Hash Extractor, software that retrieves the MD5 hash value (the digital "thumbprint") from files:[73]



iv. Privacy and other precautions

Law enforcement must avoid even any appearance of collecting intelligence or information on individuals or organizations due to religious, political, or social views, or on any other grounds that could be regarded as violating the right against discrimination. Collecting data exclusively for those reasons destroys community trust and confidence in law enforcement. Agencies must not use social media to collect information without understanding and following basic civil rights protections. Many agencies already have policies to protect civil rights and civil liberties. Agencies should include references to agency privacy protections when drafting social media policies to collect intelligence and investigate crimes.[74]

Table 8: Judicial decisions - US court precedent

SOURCE: Community of Police Services (COPS) and the Police Executive Research Forum, *Social Media and Tactical Considerations For Law Enforcement*, May 2013, p. 11.

In the United States, one key issue is whether information posted on social media sites such as Facebook is constitutionally protected as private under the Fourth Amendment, and if it is constitutionally permissible for police to set up fictitious identities in Facebook accounts or other social media in order to obtain photos, videos, and other content posted by other Facebook users.

In one case filed on August 10, 2012, the U.S. District Court for the Southern District of New York held that the government did not violate the Fourth Amendment of the USA Constitution when it accessed information from a suspect's Facebook profile that the suspect classified as "private" under the Facebook privacy settings he chose for his Facebook account[75]. The government obtained the information with the assistance

of a cooperating witness who had been "friended" by the suspect, and who thus had access to the potentially incriminating information, which included messages about past acts of violence and threats of new acts of violence against rival gang members.

"[The suspect's] *legitimate expectation of privacy ended when he disseminated posts to his 'friends' because those 'friends' were free to use the information however they wanted—including sharing it with the Government*" the court said.

Table 9: *Best Practices - Social Media policies*
See the Georgia Bureau of Investigation social media policy entitled "Guidelines for the Use of Social Media by the Investigative Division", attached as Appendix B to the Global Justice Information Sharing Initiative, *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations* (February 2013), 29–35, at www.iacpsocialmedia.org/Portals/1/documents/SMInvestigativeGuidance.pdf

2. Government agencies' databases (publicly and not-publicly available)

In many economies, local and state agencies maintain websites publicly available on-line, where general public can retrieve information, because policy, regulation, or the law permits the custodian of such information to do so. Users, and so investigators, are allowed to access hundreds of sources of current government information – such as census data, judicial decisions, property and vehicle ownership records, property ownership, lien filings, company financial reports, salaries of public employees – and a wide array of other information for which an individual has little, if any, control over its public release.[76]

Other public agencies and departments maintain registers not accessible to the general public, but may allow law enforcement agencies to access their databases, either directly, or through the appropriate administrative or judicial process.

When instant access is not guaranteed, but Courts routinely grant access, a useful practice may be that of stipulating MoUs with different government departments to such end.

Table 10: *Best practices - Brunei Darussalam ACB Intelligence Section*

SOURCE: Anti-corruption Bureau, Prime Minister's Office, Brunei Darussalam, "The Use of IT Resources for Evidence Gathering and Analysis", presented at the APEC Anti-Corruption and Transparency Working Group (ACTWG), Capacity Building Workshops on Designing Best Models on Prosecuting Corruption and Money Laundering Cases Using Financial Flow Tracking Techniques and Investigative Intelligence for Effective Conviction and Asset Recovery to Promote Regional Economic Integration, Santiago, Chile, 11-13 June 2013.

The ACB Intelligence Section has a Memorandum of Understanding for information sharing with several government departments. The mode of sharing information is by system link. The departments that have approved the MoU and the documents shared with the ACB are the following:

NO	GOVERNMENT DEPARTMENT	DOCUMENT GATHER
1	Land Transport Department	Car owners details
2	Immigration and National Registration Department	•Identity card details •Border in/out details
3	Public Service Department	Government employee management system
4	Ministry of Finance	Business registration

Financial information retrievable from public databases can be of high value for investigators. There are a great number of databases that could be used by a prosecutor or investigator in a corruption case.

Given that a suspect frequents a certain residence, for example, public records could allow investigators to ascertain the ownership of the house, when it was bought, from whom and for how much, how the payment took place and who is paying taxes on it. As for corporations, public registers permit to gather information about when and where the company was formed, who are its directors or officers, and many other data.

- **Public Databases and Records**[77]

Firearms Registries
Can provide information about liquor, firearms, and explosives licensing
Drug Enforcement Administrations
Can provide investigators with relevant case data, information on individuals and companies related to cases, known assets, business and financial information related to cases, analytical databases for the analysis of telephone number information, etc.

Financial Information Units
Can provide analytical research services, databases for evidence or leads to relationships between subjects and other persons or entities, link analysis to show connections, Suspicious Transaction Reports and many other financial information.
Tax agencies and Tax records
Can provide information on Sales and use tax, Personal property tax, Real property tax, Business license tax, Income tax, Gift tax, Inheritance tax, etc.
INTERPOL
Can provide access to international networks of criminal activity files, query by name or business name, and provide intelligence checks to complete a file.
Crime and Law Enforcement Information Centers and Networks
Provide information on criminal history, Fingerprints, Vehicles, License plates, Securities, Boats, Guns, Wanted persons (domestic and foreign), Unidentified persons files, criminal history records
Custom Service
Information on people and goods.
Companies public registries
Information on all corporations incorporated or doing business, ownership, corporate bylaws, capital, credit reports, information on corporate mergers, reorganizations and consolidations. Identification information on all partnerships and professional associations formed or doing business.
Securities Supervisors
Information about issuers, company reports and disclosures, history of dividends, stock splits, and key financial ratios; proxy statements, enforcement actions, change in registrant's certifying accountant, details of stock acquisition, source of money used to buy stock, corporate documents, documents from third parties
Bankruptcy Records
Information about bankruptcy, assets at time of bankruptcy, creditors at time of bankruptcy.
Often provides an excellent starting point for net worth purposes and leads to hidden assets
Civil and Criminal Court Records
Information on Civil suits and Criminal actions.
Can provide leads to hidden transactions or assets revealed through civil suits; leads to

witnesses who may be hostile to the subject; leads to aliases and previously unknown addresses; leads to previously unknown affiliations with other persons or entities
Divorce and Legal Separation Records
Leads to: hidden transactions or assets revealed through divorce proceedings, witnesses who may be hostile to the subject, previously unknown affiliations with other persons or entities
Automobile License Departments or Agencies
Owner's name, Vehicle identification number, Physical description of listed automobiles
Driver's License Bureau Departments or Agencies
Driver's name, date of birth, physical description, and address, License renewal date and the type of license issued
Professional and Commercial Licenses
Information about Medical, Dental, Insurance agency, Stock broker, Real estate broker, Attorney, Certified Public Accountant, Concealed weapons, Gun permits, Liquor, Notary Licenses
Real Estate Records
Building Permit records: may reveal hidden property, payments by third parties for improvements on property, leads to previously unknown affiliations with other persons or entities, evidence of beneficial ownership of the property
Grantor and Grantee Records: Deeds, Real estate agreements, Liens and lien releases, Real estate and chattel mortgages, Options to buy, Easements and easement releases.
Maps and Plats: compare county maps and plats with aerial photos, measured mileage, surveillance notes, etc.
Liens Register: may reveal new construction, property improvements, hidden property, payments by third parties for improvements on property, leads to previously unknown affiliations with other persons or entities, evidence of beneficial ownership of the property
Tax Assessor's Records: may indicate separate assessed values for land and improvement, cross reference property by legal description, who pays taxes on the property, address where the property tax bills are being sent, may cross-reference other properties whose tax bills are being sent to same address, may cross-reference other properties on which subject is paying taxes, may provide previously undisclosed relationships with other persons or entities, may provide evidence of beneficial ownership of the property
Gaming Departments or Agencies
Owners of gaming establishments, names of persons banned from gaming

establishments, financial information on gaming establishments
Civil registries
Births, Deaths, Adoptions
Trade Name Index
Trade names of businesses, including corporations, partnerships, professional corporations and sole proprietorships doing business in the region; Addresses of businesses, Name, address and identity of owners.
Bureau of Public Debt
Cash purchases of Treasury bills
Coast Guard
Records of vessels
Ministries of Interior / State Departments or similar
ID Records, Passport records, Visa records
Aviation Administration
Information on aircraft, owners and previous owners, serial number, model, information on licensed pilots
Immigration Departments
Identification information on immigrants and aliens, lists of passengers and crews on vessels from foreign ports, naturalization records, deportation records, financial statements of aliens and persons sponsoring their entry.
Postal Service
Postal money orders, Addresses, Mail covers
Trash Searches
Records obtained by searching through subject's trash
Utility Companies
Water, Sewer, Trash hauling, Electricity, Gas, Telephone.
Leads to third parties, principals, and hidden assets: may reveal third parties who are paying the bills, bills on other properties being paid by the same person or company, previously undisclosed bank accounts from which bills are being paid, leads to hidden property on which bills are being paid

CHAPTER IV. THE GATHERING OF PRIVATE DIGITAL SOURCES OF EVIDENCE AND THE USE OF DIGITAL FORENSIC TOOLS

Nowadays, large parts of human activities create some type of digital evidence.[78] Back in 2001, a study by the University of California-Berkeley already pointed out that at least 93% of all new information was created in digital format;[79] while back in 1998, 3.4 trillion e-mail messages were sent across the world.[80] Since then those figures have increased dramatically: in 2007, it was reported that more electronic documents were created worldwide in the prior year than the printed documents in all the years combined since Gutenberg invented the printing press.[81]

In 2015, 4.3 billion email accounts have been reported, including business and consumer mailboxes. The majority of email traffic comes from business emails, which account for over 100 billion emails sent and received per day.[82]

However, digital evidence is not associated only with creating an email or writing a document on a computer. Surfing the internet or driving a car with a GPS, paying bills or using a video camera, withdrawing cash or using a copy machine: each of these actions creates digital evidence, and even activities that are perceived as not producing electronic evidence are eventually digitized at some point.[83]

Significant digital sources of evidence in the investigation of corruption cases include:

Computers
Mobile devices
Removable media and external data storage devices
Online banking software
Calendar(s)
E-mail, notes, and letters
Telephone records
Financial or asset records
Electronic money transfers
Accounting or recordkeeping software

Table 11: *Hong Kong, China - How do we use IT resources?*

SOURCE: Hong Kong, China. Presentation at the APEC Anti-Corruption and Transparency Working Group (ACTWG), Capacity Building Workshops on Designing Best Models on Prosecuting Corruption and Money Laundering Cases Using Financial Flow Tracking Techniques and Investigative Intelligence for Effective Conviction and Asset Recovery to Promote Regional Economic Integration, Santiago, Chile, 11-13 June 2013.

- Data acquisition, recovery, preservation and examination
- Computer
  - Email
  - Document file…
- Mobile phone
  - Call history
  - Contact list
  - Short message
  - Email
  - Photo
  - WhatsApp

The importance of this enormous amount of evidence is that it can be recovered and used in criminal investigations, in asset tracing and in any legal proceedings. Doing so requires a process of collection, preservation and analysis of electronic data that must then be presented for use in a litigation process.

Forensic acquisition and analysis of data techniques combine lost and tampered data with other digital evidence, allowing for easier identification, collection, preservation, analysis and presentation of evidence generated or stored in a computer.[84]

Additionally, as much of the day-to-day communication and financial transactions are conducted over the Internet, real time monitoring of bank accounts, e-mail traffic and the interception and processing of other forms of on-line data become essential for conducting a proper investigation, complementing traditional investigative and surveillance techniques.[85]

Since all these activities require the assistance of a digital forensic expert, the increasing trends have led to a huge demand for highly educated specialists in these disciplines.[86]

DIGITAL EVIDENCE: Definition

Digital evidence is information and data of value to an investigation that is stored on, received, or transmitted by an electronic device. This evidence is acquired when data or electronic devices are seized and secured for examination.

NATIONAL INSTITUTE OF JUSTICE, *Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition*, U.S. Department of Justice-Office of Justice Programs, Washington, 2008, p. ix

Electronic evidence originates when electronic data regarding some type of activity or transaction are stored somewhere, where they might be accessed and recovered by a forensic examiner.

Today digital evidence can be found on everything from floppy disks to media cards, solid-state memory sticks, solid-state hard drives, cell phones, network attached storage devices, game consoles, media players, hard drives, and the "Internet cloud.

L. DANIEL – L. DANIEL, *Digital Forensics for Legal Professionals: Understanding Digital Evidence From The Warrant To The Courtroom*, Waltham, 2012, p. 5

The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

G. PALMER, *A Road Map for Digital Forensic Research*, DFRWS 16, Nov. 6, 2001

Digital Forensics makes use of different methods and techniques, in order to deal with a variety of issues and to meet the diverse needs of criminal investigations. It is possible, however, to summarize four essential elements or principles upon which every digital forensic technique relies on.[87]

Acquisition

The process of actually collecting electronic data, such as seizing a computer at a crime scene or making a forensic copy of ("acquiring" in the forensic language) a computer hard drive.

It is the first step in the forensic process and is critical to ensure the integrity of the evidence, since it is the moment where evidence is most likely to be damaged or

destroyed.

Preservation
The process of creating a chain of custody that begins prior to collection and ends when evidence is released to the owner or destroyed.
It includes keeping the evidence safe from intentional destruction by malicious persons or accidental modification by untrained personnel.

Analysis
The process of locating and collecting evidentiary items from evidence that has been collected in a case. It includes the identification of target information (such as financial records, for example) as well as the use of specific forensic tools.

Presentation
The activity of presenting the examiner's findings is the last step in the process of forensic analysis of electronic evidence. This includes not only the written findings or forensic report, but also the creation of affidavits, depositions of experts, and court testimony.

Table 12: *Hong Kong, China - Challenges*

SOURCE: Hong Kong, China. Presentation at the APEC Anti-Corruption and Transparency Working Group (ACTWG), Capacity Building Workshops on Designing Best Models on Prosecuting Corruption and Money Laundering Cases Using Financial Flow Tracking Techniques and Investigative Intelligence for Effective Conviction and Asset Recovery to Promote Regional Economic Integration, Santiago, Chile, 11-13 June 2013.

<u>Technical difficulties</u>

- Cloud computing
  - Information and evidence are remotely stored
  - Liaison with online service providers
- Huge data size
  - Storage Area Network (SAN) to keep forensic image
- Data encryption
  - Password cracking tool
  - Chip level data acquisition

Admissibility of digital evidence

- Local digital evidence
- Foreign digital evidence
- Expert opinion on chain of evidence
- Admissibility of evidence in court trials

A. Best practices for handling digital evidence

In dealing with digital evidence, law enforcement agencies must ensure that adequate procedures are in place, since every activity of the law enforcement personnel exposes the evidence to the risk of accidental modification. That's the reason why, in ensuring that evidence will be accepted in a court of law as being authentic and an accurate representation of the original evidence, the moments of collection and preservation of evidence are extremely critical.

Modification of evidence can have a devastating effect on the entire case, and therefore digital evidence needs to be protected and preserved all along the process collection, acquisition, analysis and presentation.

In the implementation of proper procedures and in the elaboration of training programs, agencies must apply the following general forensic principles:[88]

- The process of collecting, securing, and transporting digital evidence should not change the evidence;
- Digital evidence should be examined only by those trained specifically for that purpose;
- Everything done during the seizure, transportation, and storage of digital evidence should be fully documented, preserved, and available for review.

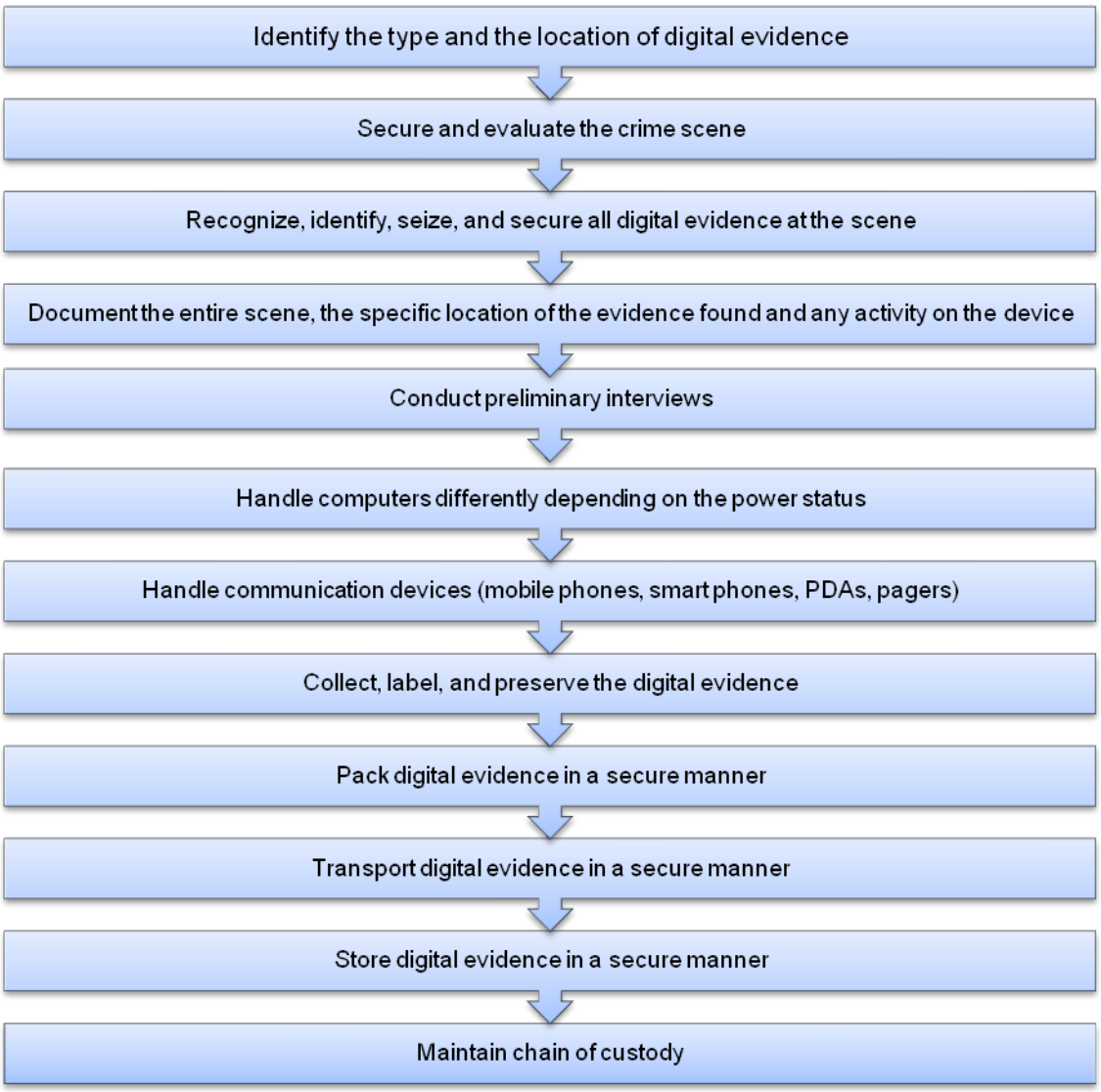
In the following sections, models are presented of those protocols and procedures that every agency should put in place for each critical stage in the digital evidence gathering process.[89]

1. Collection and preservation of digital evidence

The collection step is critical since this is the first real contact with evidence. Not following proper collection procedures can lead to the destruction or modification of evidence, lost evidence, and subsequent challenges of the evidence collected.[90] Some

digital evidence requires special collection, packaging, and transportation techniques. Indeed, data can be damaged or altered by electromagnetic fields such as those generated by static electricity, magnets, radio transmitters, and other devices.[91]

The following chart summarizes all activities that must be performed in the process of acquisition. Each activity will be detailed below.



1	Identify the type and the location of digital evidence
☐	Include any location and item in which digital evidence may reside in preparing or applying for a search warrant.
☐	Determine the necessary equipment to take to the scene
☐	Review the legal authority to collect evidence, ensuring any restrictions are noted.

Warning

Collecting items not previously identified can cause that evidence to be suppressed in a legal action. Identification language must be specific and must have correct terminology; using language such as “CPU” instead of computer would mean that you can collect only the Central Processing Unit of a computer and not the computer itself.

2 Secure and evaluate the crime scene

- ☐ Follow departmental policy for securing crime scenes.
- ☐ Ensure that no unauthorized person has access to any electronic devices at the crime scene.
- ☐ Refuse offers of help or technical assistance from any unauthorized persons.
- ☐ Remove all persons from the crime scene or the immediate area from which evidence is to be collected.

3 Recognize, identify, seize, and secure all digital evidence at the scene

- ☐ Search the scene systematically and thoroughly;
- ☐ Immediately secure all electronic devices, including personal or portable devices.
- ☐ Ensure that the condition of any electronic device is not altered.
- ☐ Leave a computer or electronic device off if it is already turned off.
- ☐ Consider the possibility of anti-forensic techniques (such as destructive devices and wiping software)

4 Document the entire scene

- ☐ Record the location of the scene, the state, power status, and condition of computers, storage media, wireless network devices, mobile phones, smart phones, PDAs, and other data storage devices; Internet and network access; and other electronic devices;
- ☐ Photograph the evidence in place prior to collection or duplication;
- ☐ Prepare a complete inventory of each item including identifying information such as serial numbers, manufacturer, and descriptions;
- ☐ Record all activity and processes on display screens

- ☐ Record all physical connections to and from computers
- ☐ Record any network and wireless access point that may be present
- ☐ Do not move electronic devices until they are powered off

5 Conduct preliminary interviews

In conformity with applicable laws and regulations, investigators should ask all adult persons of interest at the crime scene for the following information:

- ☐ Names of all users of the computers and devices.
- ☐ All computer and Internet user information.
- ☐ All login names and user account names.
- ☐ Purpose and uses of computers and devices.
- ☐ All passwords.
- ☐ Any automated applications in use.
- ☐ Type of Internet access.
- ☐ Any offsite storage.
- ☐ Internet service provider.
- ☐ Installed software documentation.
- ☐ All e-mail accounts.
- ☐ Security provisions in use.
- ☐ Web mail account information.
- ☐ Data access restrictions in place.
- ☐ All instant message screen names.
- ☐ All destructive devices or software in use.
- ☐ MySpace, Facebook, or other online social networking Web site account information.

☐	Any other relevant information

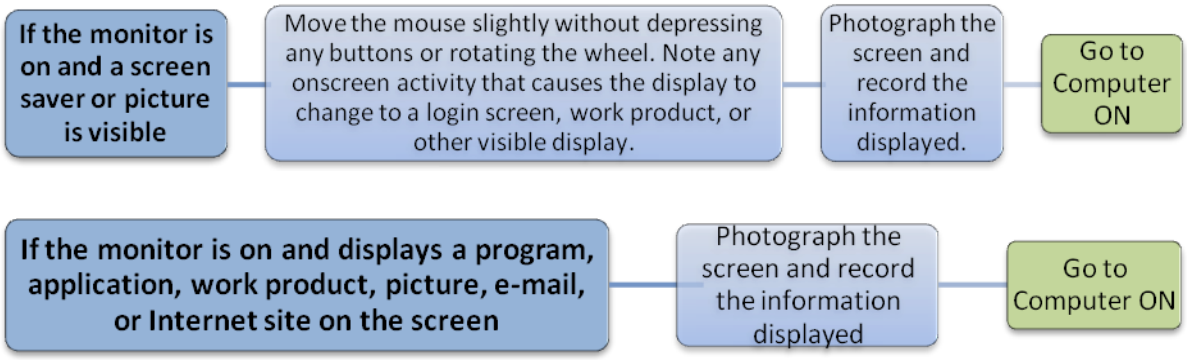
6 Handle computers differently depending on the power status

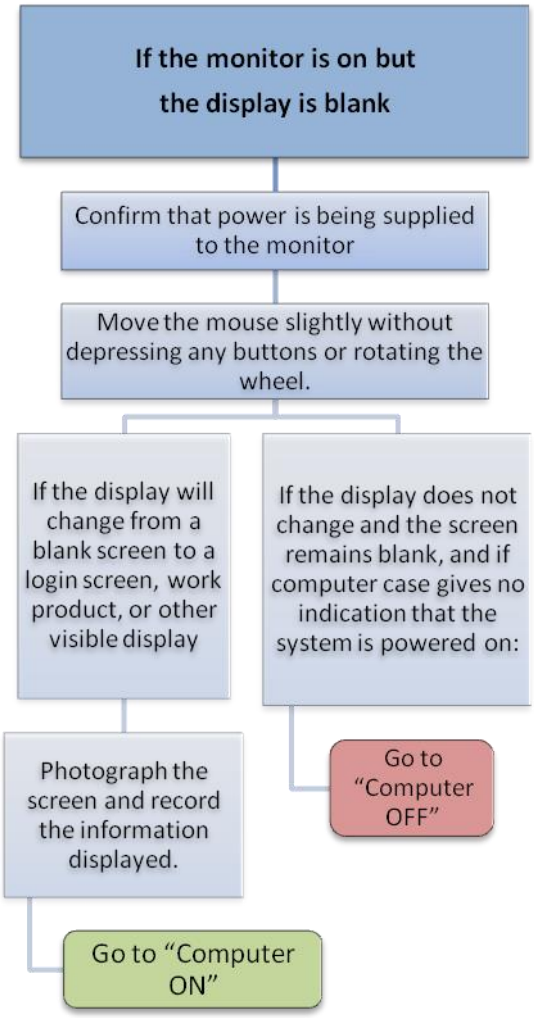
If someone attempts to collect a device and does not understand the proper methods to shut down the computer, operates the computer prior to shutdown, or shuts down a critical business server improperly, it can lead to data loss, civil liability for lost business, and the loss of critical evidence that could be collected prior to shut down.

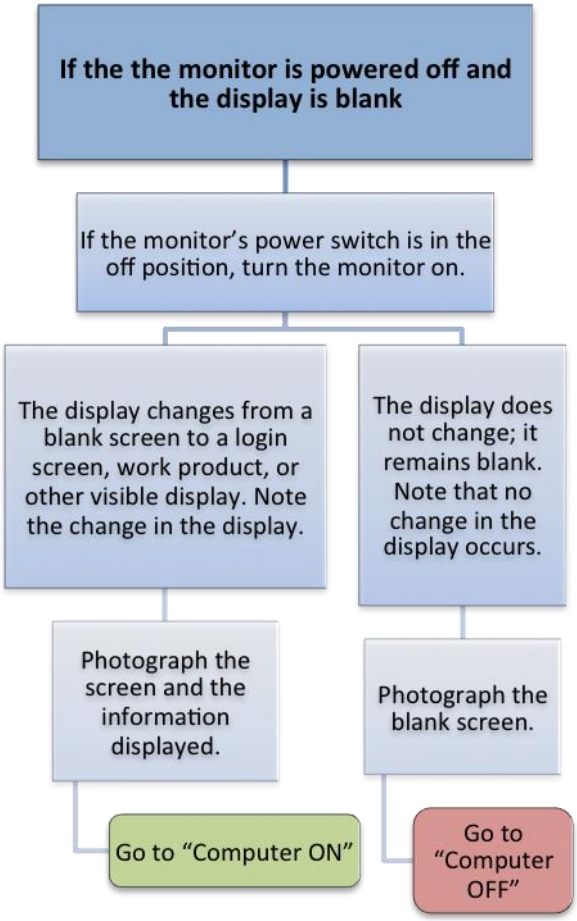
6.1 Assess the Situation

☐	Look and listen for indications that the computer is powered on. Listen for the sound of fans running, drives spinning, or check to see if light emitting diodes (LEDs) are on.
☐	Check the display screen for signs that digital evidence is being destroyed. Words to look out for include “delete,” “format,” “remove,” “copy,” “move,” “cut,” or “wipe.”
☐	Look for indications that the computer is being accessed from a remote computer or device.
☐	Look for signs of active or ongoing communications with other computers or users such as instant messaging windows or chat rooms.
☐	Take note of all cameras or Web cameras (Web cams) and determine if they are active
☐	Look and listen for indications that the computer is powered on. Listen for the sound of fans running, drives spinning, or check to see if light emitting diodes (LEDs) are on.

6.2 Identify the computer’s power status




If the monitor is on but the display is blank
Confirm that power is being supplied to the monitor
Move the mouse slightly without depressing any buttons or rotating the wheel.
If the display will change from a blank screen to a login screen, work product, or other visible display
If the display does not change and the screen remains blank, and if computer case gives no indication that the system is powered on:
Photograph the screen and record the information displayed.
Go to "Computer OFF"
Go to "Computer ON"



6.3	**Computer OFF**
	For desktop, tower, and minicomputers follow these steps:
☐	Document, photograph, and sketch all wires, cables, and other devices connected to the computer.
☐	Uniquely label the power supply cord and all cables, wires, or USB drives attached to the computer as well as the corresponding connection each cord, cable, wire, or USB drive occupies on the computer.
☐	Photograph the uniquely labeled cords, cables, wires, and USB drives and the corresponding labeled connections.
☐	Remove and secure the power supply cord from the back of the computer and from the wall outlet, power strip, or battery backup device.
☐	Disconnect and secure all cables, wires, and USB drives from the computer and document the device or equipment connected at the opposite end.
☐	Place tape over the floppy disk slot, if present.

☐	Make sure that the CD or DVD drive trays are retracted into place; note whether these drive trays are empty, contain disks, or are unchecked; and tape the drive slot closed to prevent it from opening.
☐	Place tape over the power switch.
☐	Record the make, model, serial numbers, and any user-applied markings or identifiers.
☐	Record or log the computer and all its cords, cables, wires, devices, and components according to agency procedures.
☐	Package all evidence collected following agency procedures to prevent damage or alteration during transportation and storage.
	For laptop computers follow these steps:
☐	Document, photograph, and sketch all wires, cables, and devices connected to the laptop computer.
☐	Uniquely label all wires, cables, and devices connected to the laptop computer as well as the connection they occupied.
☐	Photograph the uniquely labeled cords, cables, wires, and devices connected to the laptop computer and the corresponding labeled connections they occupied.
☐	Remove and secure the power supply and all batteries from the laptop computer.
☐	Disconnect and secure all cables, wires, and USB drives from the computer and document the equipment or device connected at the opposite end.
☐	Place tape over the floppy disk slot, if present.
☐	Make sure that the CD or DVD drive trays are retracted into place; note whether these drive trays are empty, contain disks, or are unchecked; and tape the drive slot closed to prevent it from opening.
☐	Place tape over the power switch.
☐	Record the make, model, serial numbers, and any user applied markings or identifiers.
☐	Record or log the computer and all its cords, cables, wires, devices, and components according to agency procedures.
☐	Package all evidence collected following agency procedures to prevent damage or alteration during transportation and storage.

6.4 Computer ON

For practical purposes, removing the power supply when you seize a computer is generally the safest option. If evidence of a crime is visible on the computer display, however, you may need to request assistance from personnel who have experience in volatile data capture and preservation.

☐	Examine the computer for any running processes. If it is observed running a destructive process, the examiner should stop the process and document any actions taken.
☐	Consider Capture RAM and other volatile data from the operating system (**See Box below**)
☐	Determine if any of the running processes are related to cloud or off-site storage. When encountered, the examiner should coordinate with the appropriate legal authority to ensure the scope covers the off-site acquisition.
☐	Document and hibernate any running virtual machines.
☐	Consider the potential of encryption software installed on the computer or as part of the operating system. If present, appropriate forensic methods should be utilized to capture the unencrypted data before the computer is powered off.
☐	Save any opened files to trusted media.
☐	Isolate the computer from any network connectivity.
☐	Use a triage tool to preview data.
☐	Evaluate the impact of pulling the plug vs. shutting the computer down. This is typically dependent upon the operating system and file system encountered.
	In the following situations, immediate disconnection of power is recommended
■	Information or activity onscreen indicates that data is being deleted or overwritten.
■	There is indication that a destructive process is being performed on the computer's data storage devices.
■	The system is powered on in a typical Microsoft ® Windows ® environment. Pulling the power from the back of the computer will preserve information about the last user to login and at what time the login occurred, most recently used documents, most recently used commands,
	In the following situations, immediate disconnection of power is NOT recommended:
■	Data of apparent evidentiary value is in plain view onscreen. The first responder should seek out personnel who have experience and training in capturing and preserving volatile data before proceeding.
■	Indications exist that any of the following are active or in use:
	○ Chat rooms and instant message windows
	○ Open text documents
	○ Remote data storage
	○ Data encryption
	○ Financial documents

For mainframe computers, servers, or a group of networked computers, the first responder should secure the scene and request assistance from personnel who have training in collecting digital evidence from large or complex computer systems.

Table 13: *Volatile Data*

SOURCE: Digital Forensics for Legal Professionals: Understanding Digital Evidence From The Warrant To The Courtroom, Waltham, 2012, p. 26.

Some evidence is only present while a computer or server is in operation and is lost if the computer is shut down. Evidence that is only present while the computer is running is called volatile evidence and must be collected using live forensic methods. This includes evidence that is in the system's RAM (Random Access Memory), such as a program that only is present in the computer's memory. These programs are considered TSRs or Terminate and Stay Resident programs. […] There are also many types of other volatile evidence that are only available while the computer is running, including certain temporary files, log files, cached files, and passwords. RAM is cleared when the computer is turned off and any data that is present is lost. This can be a critical step if there is suspicion that any kind of data encryption is enabled that prevents the hard drive or portions of the hard drive from being viewed. In many cases the only way to recover the password needed to remove the encryption on a hard drive is to collect the "live memory" before the computer is turned off. Also, if the computer is running, the encrypted portion of the data storage would be accessible, but only until the computer is turned off, making it essential that the hard drive is copied while the computer is still turned on. There are tools available to make copies of RAM and hard drives on running computers and line-of-business servers that cannot be shut down, and still ensure that those copies are forensically sound.

Table 14: *Warning - Acquire data from live systems*

SOURCE: Scientific Working Group on Digital Evidence (SWGDE), Capture of Live Systems, 2008, p. 2.

Great care must be taken when attempting to capture or acquire data from live systems. These are advanced techniques that require advanced training and tools to accomplish the desired results while minimizing the possible destruction of data or hardware. If the person attempting to acquire the data is unsure of the methods used to perform the acquisition, then professional assistance should be sought.

There are three methods utilized in live acquisitions:

1. RAM dump

2. Logical copying of files

3. Physical acquisition of the entire system

Each of these can be used independently or in conjunction with others depending on the scope of the search.

7 Communication devices (mobile phones, smart phones, PDAs, pagers)

☐	Secure the devices
☐	Prevented devices from receiving or transmitting data once they are identified and collected as evidence

8 Collect, label, and preserve the digital evidence

☐	Tag each item for tracking and identification.
☐	Secure each item to prevent inadvertent operation. This includes placing tamper-proof tape over power outlets, CD-ROM drives, USB ports, and floppy disk trays.
☐	Bag each item in a forensically sound manner, into a secure container that is sealed with tamper-proof tape to ensure that the evidence is not modified or damaged during transport.
☐	If more than one computer is seized as evidence, all computers, cables, and devices connected to them should be properly labeled to facilitate reassembly if necessary.

9 Pack digital evidence in a secure manner

☐	Ensure that all digital evidence collected is properly documented, labeled, marked, photographed, video recorded or sketched, and inventoried before it is packaged. All connections and connected devices should be labeled for easy reconfiguration of the system later.
☐	Remember that digital evidence may also contain latent, trace, or biological evidence and take the appropriate steps to preserve it. Digital evidence imaging should be done before latent, trace, or biological evidence processes are conducted on the evidence.
☐	Pack all digital evidence in antistatic packaging. Only paper bags and envelopes, cardboard boxes, and antistatic containers should be used for packaging digital evidence. Plastic materials should not be used when collecting digital evidence because plastic can produce or convey static electricity and allow humidity and condensation to develop, which may damage or destroy the evidence.
☐	Ensure that all digital evidence is packaged in a manner that will prevent it from being bent, scratched, or otherwise deformed.
☐	Leave cellular, mobile, or smart phone(s) in the power state (on or off) in which they were found.
☐	Package mobile or smart phone(s) in signal-blocking material such as faraday isolation bags, radio frequency-shielding material, or aluminum foil to prevent data messages from being sent or received by the devices.
☐	Collect all power supplies and adapters for all electronic devices seized.

10	Transport digital evidence in a secure manner
☐	Specific care should be taken with the transportation of digital evidence to avoid physical damage, vibration and the effects of magnetic fields, electrical static and large variations of temperature and/or humidity.
☐	Keep digital evidence away from magnetic fields such as those produced by radio transmitters, speaker magnets, and magnetic mount emergency lights.
☐	Avoid keeping digital evidence in a vehicle for prolonged periods of time. Heat, cold, and humidity can damage or destroy digital evidence.
☐	Ensure that computers and electronic devices are packaged and secured during transportation to prevent damage from shock and vibration.
☐	Document the transportation of the digital evidence and maintain the chain of custody on all evidence transported.

11	Store digital evidence in a secure manner
☐	Ensure that the digital evidence is inventoried in accordance with the agency's policies.
☐	Ensure that the digital evidence is stored in a secure, climate-controlled environment or a location that is not subject to extreme temperature or humidity.
☐	Ensure that the digital evidence is not exposed to magnetic fields, moisture, dust, vibration, or any other elements that may damage or destroy it.
	WARNING: Potentially valuable digital evidence including dates, times, and system configuration settings may be lost due to prolonged storage if the batteries or power source that preserve this information fails. Where applicable, inform the evidence custodian and the forensic examiner that electronic devices are battery powered and require prompt attention to preserve the data stored in them.

12	Maintain chain of custody
☐	Proper check-in and check-out procedures with a maintained chain of custody for any access to or movement of the evidence
☐	Final disposition of the evidence, recorded in the chain of custody for any evidence that is released or destroyed
☐	Each piece of evidence should be protected from damage or alteration, labeled and a chain-of-custody maintained as determined by organizational policy.
☐	Document the transportation of the digital evidence and maintain the chain of custody on all evidence transported.

Table 15: *Best Practices –Hong Kong China - Faraday Bags*

SOURCE: Hong Kong, China. Presentation at the APEC Anti-Corruption and Transparency Working Group (ACTWG), Capacity Building Workshops on Designing Best Models on Prosecuting Corruption and Money Laundering Cases Using Financial Flow Tracking Techniques and Investigative Intelligence for Effective Conviction and Asset Recovery to Promote Regional Economic Integration, Santiago, Chile, 11-13 June 2013.

Mobile devices such as smart phones are kept in radio frequency shielding faraday bags to prevent digital evidence from being interfered with by external communication.

2. Acquisition of digital evidence

Acquisition is the part of the forensic process during which actual data is copied or duplicated. Once again, ensuring the integrity of evidence is the most critical part of the procedure.

a. Duplication

The only accepted method for duplicating electronic evidence requires that the original be protected from any possibility of alteration during the duplication process. This requires the use of accepted tools and techniques that allow the duplication of the evidence in a forensically sound manner.

Forensic methods for duplication

The proper forensic method for duplicating evidence from a computer hard drive or other media storage device requires the use of write-blocking of the original storage device.

Write-blocking can be accomplished either by using a physical hardware device that is

connected between the original (source) and the copy (target) hard drive or by using a special boot media that can start a computer in a forensically sound manner.

When is practical to remove the hard drive:

- ☐ Remove the hard drive from the computer
- ☐ Connect it to a physical write-blocker
- ☐ Use a forensic workstation and forensic software to make the copy.

In case it is not practical to remove the hard drive:

- ☐ Start up the computer in a forensically sound manner (see next box)
- ☐ Make a copy of the hard drive using a software-based write-blocking method

Table 16: Starting up a computer with a forensic operating system

SOURCE: DANIEL – L. DANIEL, Digital Forensics for Legal Professionals: Understanding Digital Evidence From The Warrant To The Courtroom, Waltham, 2012, p. 31.

When a computer is first turned on, it goes through a set of steps, beginning with a Power On Self-Test (POST), followed by loading of the Basic Input Output System (BIOS).

During normal operation, the computer will load the operating system installed on the hard drive, such as Microsoft Windows or the Mac OS. It is possible to prevent the computer from loading the operating system that is installed on the hard drive.

When preparing to perform a forensic copy of a computer's hard drive(s), a forensic examiner would force the computer to load a special forensic operating system from a specially prepared boot media.

This is critical because when a computer starts up (boots) normally from the installed operating system, whether Windows or Mac OS or Linux, these operating systems automatically "mount" the hard drive(s) in read/write mode. […] These forensic operating systems are modified to effectively turn off the ability of the computer to make any changes to the hard drive(s).

Table 17: *Why not to use a non-forensic duplication method*

SOURCE: DANIEL – L. DANIEL, Digital Forensics for Legal Professionals: Understanding Digital Evidence From The Warrant To The Courtroom, Waltham, 2012, p. 30.

Using non forensic methods will always lead to modification of the original evidence and/or incomplete copies of the original evidence that cannot be verified using forensic methods.

Personnel not trained in the proper forensic methods for duplicating electronic

evidence may start a computer up and then make copies of the data on the hard drive.

When a computer is started up in this manner, the operating system can write to the hard drive and change file dates, change log files, and other types of files, effectively modifying and destroying critical evidence.

b. Verification

This is the final step in the forensic copy process. In order for evidence to be admissible, it must be possible to verify that the evidence presented is exactly the same as the original collected.

Table 18: *Creating a "hash value"*

SOURCE: DANIEL – L. DANIEL, Digital Forensics for Legal Professionals: Understanding Digital Evidence From The Warrant To The Courtroom, Waltham, 2012, p. 31.

Verification is accomplished by using a mathematical algorithm that calculates a number based on the contents of the evidence. … This is called creating a "hash value" and is performed by using either the Message Digest 5 (MD-5) algorithm or a Secure Hash Algorithm (SHA). The MD-5 is the most commonly used method for verification in computer forensics at this time. Forensic duplication tools automatically create a "verification" hash for the original and the copy during the duplication process. If these hash values do not match, there is an opening for a challenge to the authenticity of the evidence as compared to the original.

Table 19: *Best Practices - The Indonesian Experience of KOMISI PEMBERANTASAN KORUPSI*

SOURCE: Indonesia presentation at the APEC Anti-Corruption and Transparency Working Group (ACTWG), Capacity Building Workshops on Designing Best Models on Prosecuting Corruption and Money Laundering Cases Using Financial Flow Tracking Techniques and Investigative Intelligence for Effective Conviction and Asset Recovery to Promote Regional Economic Integration, Santiago, Chile, 11-13 June 2013.

We include a digital fingerprint in our affidavit when we seize the evidence. This policy is taken to strengthen the validity of the evidence. Thus, the validity of the evidence can be tested by everyone.

KOMISI PEMBERANTASAN KORUPSI
REPUBLIK INDONESIA

"Untuk Keadilan"

BERITA ACARA PENGAMBILAN DATA ELEKTRONIK

-------- Pada hari ini Selasa tanggal Lima bulan Mei dua ribu Sembilan (05-05-2009), saya penyidik Komisi Pemberantasan Korupsi : ----------

1 Nama : Adi Deriyan Jayamarta
Jabatan : Penyidik pada KPK

Bersama – sama dengan : ----------

2. Nama : Agus Ariwibowo
Jabatan : Penyidik pada KPK

Berdasarkan : ----------

1. Laporan Kejadian Tindak Pidana Korupsi Nomor : LKTPK-09/KPK/IV/2009 tanggal 27 April 2009.----------
2. Surat Perintah Penyidikan Nomor : Sprin.Dik-14/01/IV/2009 tanggal 28 April 2009.----------
3. Penetapan Pengadilan Negeri Jakarta Pusat Nomor : 22/Pen.Pid/2009/PN.JKT.PST. tanggal 30 April 2009.----------
4. Surat Perintah Penggeledahan Nomor : Sprin.Dah - 13/01/IV/2009 tanggal 30 April 2009.------

Telah melakukan pengambilan data elektronik : ----------

Dari Lantai 12, NETWAY :

1. Data dari Hardisk merk **MAXTOR**, S/N: **2HB2338T**, kapasitas **320 GB**, pengguna/penguasa barang: **JULIANITA N**, jabatan: Sekretaris Direktur Operasional dengan nilai MD5 Hash: **52C610C9BBF030F5D64FD82CC00B198E**

2. Data dari Flashdisk merk **MY FLASH** , S/N: **F786007268E17C**, kapasitas **256 GB** , pengguna/penguasa barang: **JULIANITA**, jabatan: Sekretaris Dirut Operasional dengan nilai MD5 Hash: **3C508DD8F8B2BD7DBC828281EA1D61F3**

3. Data dari Hardisk merk **SEAGATE** Tipe **ST380011A**, S/N: **4JV8167Z**, kapasitas **80 GB** dari Komputer Desktop dengan SN MotherBoard : **05CK020-06589-60-MBL2L0-A01** , pengguna/penguasa barang: **JULIANITA**, Jabatan: Sekretaris Dirut Operasional dengan nilai MD5 Hash: **31A55C69C07C8E62AC6AEE8F4C12D427**

4. Data dari Hardisk Laptop Merk **ACER ASPIRE 3620** dengan SN : **LXAA60C0686130929CKS00** , pengguna/penguasa barang: **NAFNEET**, dengan nilai MD5 Hash: **D9E736047438E25E4C2E1394A29EC6FD**

5. Data dari Hardisk merk **SEAGATE** Tipe **ST3802110A**, S/N: **4LR1G299**, kapasitas **80 GB** dari Komputer Desktop dengan SN MotherBoard : **058K14500684-604ABL2L0-A01** , pengguna/penguasa barang: **RAHMANITA**, jabatan: Staf keuangan dengan nilai MD5 Hash: **AC002296BD8FA084C3525DE2C39B4D89**

Table 20: Case example – *Pronosticos* case, the Mexican Experience

SOURCE: Mexico presentation at the APEC Anti-Corruption and Transparency Working Group (ACTWG), Capacity Building Workshops on Designing Best Models on Prosecuting Corruption and Money Laundering Cases Using Financial Flow Tracking Techniques and Investigative Intelligence for Effective Conviction and Asset Recovery to Promote Regional Economic Integration, Santiago, Chile, 11-13 June 2013.

Six public servants at *Pronósticos Deportivos*, a national lottery branch, defrauded the institution for about 110 million pesos. The investigation unit (DGII) investigated the modus operandi and fully identified them.

Computer forensics performed actions:

Phase 1

Forensics procedures were applied, like data recovery from computer hard disks where the videos were recorded and edited to manipulate the lottery results.

Phase 2

Forensics procedures were also applied to the surveillance system to get the videos from the day the fraud was made.

Phase 3

The videos were checked sequentially to identify how the public servants managed to trick the results and those results were reported as evidence to ministerial authority.

Results:

- ✓ The fraud and the modus operandi to simulate the lottery results were detected.
- ✓ Computer forensics analysis helped to get stronger evidence against the public servants, in order to impose administrative and financial penalties.
- ✓ By the other hand, preliminary inquiry was strengthened through computers forensics analysis and criminal actions were prosecuted by the corresponding judicial authorities.
- ✓ As it was said before, the findings obtained from the computer forensics analysis yielded sufficient evidence for the judicial authority to determine the impound of bank accounts, where were deposited the economic resources that were fraudulently obtained, up to an amount of $ 110,000,000 million MXN.

B. Single types of digital evidence

1. Hash Values

The hash value is the result of a mathematical algorithm performed against a file or a hard drive. It is a unique digital thumbprint of the file or the hard drive as it exists at the time of the hashing process. There exist two types of hashes, MD5 and SHA1, both serving the same functions:

Hash value functions in digital forensic:
To verify that a forensic image of digital evidence is exactly the same of the original
To find hidden files in a computer, when the hash value of the original file is known
To determine whether a file with a known hash value exists on a computer

2. Metadata

Metadata is stored information about another data. It can be very useful for investigators, since it allows them to know a variety of information about a file, such as authorship, editing time, the machine on which the file was created.

Metadata is usually stored in:
Electronic Document
Picture
Webpage
Browser
File system

3. E-mail

Nowadays, e-mail is one of the most abundant forms of evidence available for investigators. This is essentially due to a series of factors: (i) most people use e-mail informally and candidly; (ii) many people believe that e-mail messages are impermanent; (iii) e-mails are more difficult to get rid of than most users believe, because of the ease of copying and forwarding, the fact that most e-mail systems

require a two-step process to permanently delete e-mail from a system, and that the undeleted e-mails may be captured on system backups.[92]

E-mail is defined as a «document created or received on an electronic mail system including brief notes, more formal or substantive narrative documents, and any attachments, such as word processing and other electronic documents, which may be transmitted with the messages.»[93]

Information that can be retrieved
Content of the e-mail
Identification of the sender
Location of the sender
Identification of the consignee

Emails can be stored in multiple and different places, depending on the type of account, providing multiple opportunities for investigators to recover email even when they have been someway deleted.[94]

Email Servers
Corporate e-mail accounts They are typically hosted on a mail server, such Microsoft Exchange or Lotus Notes. These mail servers are usually backed up on a regular basis on tape or disk, while additional backups may be available at remote locations via off-site storage applications.
Free e-mail accounts Are hosted by companies who are in the business of marketing via the Internet. Today the biggest providers are Google Mail, Yahoo Mail and Microsoft Hotmail, even though many other free e-mail account providers are available to the public.
Internet Service Providers (ISPs) Provide e-mail accounts as part of the service when customers sign up for an account. These range from local ISPs who provide dial-up services in rural areas to high-speed Internet providers via DSL, cable, or satellite.
Note: It is possible to get email messages from email internet providers via search warrant. Even though it varies by service providers, usually emails deleted by users are purged from the provider servers on a regular basis.

Personal Devices
Computers Emails are stored in different formats trough several software that might be installed on the computer, such as Microsoft Outlook (file .pst), Outlook express (file .dbx), Apple mail (file .mbox). Even the use of a browser to navigate web –based mail account allows investigators to recover the emails that are cached on the hard drive as web pages.
Cell Phones, Tablets and Pad Computers The operating system of portable devices provides for email client programs which makes readable email that are stored in the memory of the device.

Table 21: Best practices

The United States Experience - Challenges Associated with Obtaining and Utilizing the Content of Electronic Mail

SOURCE: The United States presentation at the APEC Anti-Corruption and Transparency Working Group (ACTWG), Capacity Building Workshops on Designing Best Models on Prosecuting Corruption and Money Laundering Cases Using Financial Flow Tracking Techniques and Investigative Intelligence for Effective Conviction and Asset Recovery to Promote Regional Economic Integration, Santiago, Chile, 11-13 June 2013.

How does this help in financial investigations?

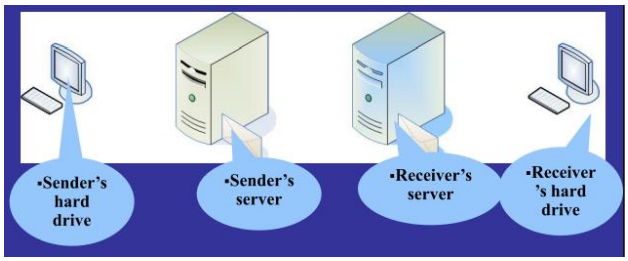
- Subject may have bank statements sent to their email address.
- Subject may be directing the movement of criminal proceeds by email.
- Communication between facilitators, and money launderers.

ECPA and Email

- Electronic Communications Privacy Act limits the United States' ability to obtain email evidence.

Where is someone's e-mail?

- Four copies, in different places
- Usually search the receiver's server



What do we search?

Where is their server?

• Domain name system

Content available by search warrant

- To/From
- Attachments
- Subject Line
- Content of Messages
- IP Addresses

4. Cell phones and Cellular Systems

The usage of cell phones by suspects may allow investigators to retrieve a variety of information and potential forms of evidence, such as:

Data stored on the phone
Text messages, contact list, call history, pictures and any other type of document can be stored on cellphones. There exist three forensic methods to retrieve them:
▪ Physical acquisition: performed using a forensic software, is the best option since it allows to get all the types of data. It is not always possible.
▪ Logical acquisition: also performed using a forensic software, it is the second option since do not allow to recover every type of data.
▪ Manual acquisition: performed by an examiner who navigates the cell phone while takes picture of the screen, it is the last option when previous seen methods are not available.

Call detail records
Cellular service providers use derived information in call detail records for use in their billing, coverage and analytics, such as:
▪ The date the call was made or received
▪ The time the call was made or received
▪ The number called/calling
▪ Usage type(voice, data, SMS, MMS)

Cell phone location
Even though a cell phone record cannot exactly locate the phone, it is possible to place the phone within a general area, corresponding to the radius of coverage of the cell tower that was connected to the phone in a specific moment.

5. Accounting software

Individuals and business use accounting programs, i.e. a software designed to manage the financial resources and to keep track of the money.

Personal accounting software
Allows individuals to manage personal money and home finances. These programs can reveal a lot of useful information about financial habits of the user. Since they can synchronize with the person bank, these type of programs allow investigators to retrieve bank accounts' information without ask for them to bank.

Business accounting software
Small, medium and multinational companies make use of accounting software to manage the money and to keep an audit trail that can be used to store information about every transaction.

c. Digital Forensic Tools

The following is a list of useful forensic tools[95]:

Forensic Suites (multiple tasks: acquisition, verification, analysis, preservation)
▪ EnCase (Guidance Software Corporation)
▪ FTK Forensic Tool Kit (Access Data Corporation)
▪ iLook LEO and iLookPI (Perlustro Corporation)
▪ SMART (ASR Data, Data Acquisition and Analysis, LLC)
▪ P2 Commander (Paraben Corporation)
▪ X-Ways Forensics (X-Ways Software Technology AG)
▪ MacForensicsLab (MacForensicsLab, Inc.)
▪ BlackLight Mac Analysis (BlackBag Technologies)
Acquisition Software
▪ EnCase Forensic Software (Guidance Software Corporation)
▪ Linen (Guidance Software Corporation)
▪ FTK Imager (Access Data Corporation)
▪ Forensic Replicator (Paraben Corporation)

▪ MacQuisition (BlackBag Technologies)
▪ Helix (e-fense)
Acquisition hardware devices
▪ Tableau
▪ Logicube
▪ Weibetech
▪ Intelligent Computer Solutions
▪ Voom Technologies
E-mail
▪ Email Examiner and Network Email Examiner (Paraben Corporation)
▪ Email Detective (Hot Pepper Technology)
▪ Mail Analyzer (Belkasoft)
Chat Programs
▪ Forensic software designed to recover chat logs from chat services such as Skype and others.
▪ Forensic IM Analyzer (Belkasoft)
▪ Chat Examiner (Paraben Corporation)
Internet History
▪ NetAnalysis (Digital Detective)
▪ Browser Analyzer (Belkasoft)
Mobile device
▪ Paraben Device Seizure (Paraben Corporation)
▪ Cellebrite (Cellebrite USA Corporation)
▪ Susteen SecureView (Susteen Inc.)
▪ CellDEK (Logicube)
▪ Mobilyze (BlackBag Technologies)
▪ BitPim (Open source free application)
▪ XRY (Micro Sysemation AB)
▪ Berla Corp GPS Forensic Software (Berla Corporation)

CHAPTER V. HUMAN INTELLIGENCE

People are a rich source of information in any investigation, since the very object of investigations is always the human behavior. This is the reason why intelligence derived from information collected and provided by human sources is essential in every kind of investigation, and why, even in the digital era, human intelligence sources remain one of the key operational tools for law enforcement agencies.

A. Suspect profiling

When planning an investigation into a possible criminal conduct committed by an individual or a corporation, it is essential to identify the key information – and the related key questions –that are needed to set the ground for a deeper comprehension of the alleged facts and the suspect's profile, as well as to further develop the case.

Identifying key questions and target information is critical in order to establish a priority order among the sources of information to be consulted and the investigative actions to be taken. This also allows channeling the limited resources only to those selected leads which may result in the development of the most significant evidence in a timely manner.

Basic information can be organized into six categories, corresponding to six key questions about the alleged facts under investigation.[96]

Who?	
☐	Full name, plus any other identifying personal particulars, such as date of birth, current address, aliases, nicknames
☐	Criminal records reference number, or other adverse records, including previous intelligence traces
☐	Nationality, ethnicity, immigration status, language(s) and dialect(s)
☐	Family members, and the extent of their involvement

What?	
☐	Main criminal activities, other criminal activities
☐	Scale and frequency of criminal activities
☐	Nature of involvement, role
☐	Associates and contacts, including the nature of the relationships- 'Legitimate' business activities

Where?	
☐	Main locations of criminal activities, plus reach (‘turf’) or spread
☐	Use of vehicles and other means of transport, including driving licence details and vehicle registration numbers
☐	Travel details, including passport details, routes

When?	
☐	Actual dates, times
☐	Periods (from/to)

How?	
☐	Criminal methods (how the business is organized and conducted)
☐	Means of communication, including telephone numbers, Internet use, use of coded language
☐	Assets employed (e.g., premises, vehicles, personnel)

Why?	
☐	Rationale for particular actions and choices
☐	Motivation
☐	Attitudes (e.g., towards risk, criminal opportunities)
☐	Lifestyle (use of criminal profits to fund property purchases, vehicles, ‘nesteggs’, family support, entertainment, holidays, etc.)

When dealing with suspects of corruption, investigators should focus on those elements that have proven to be common in the stipulation and execution of a corrupt agreement.

The Briber: Private individual or entity	
☐	All official data on the company: Trade Register; Stock Exchange
☐	Organizational charts for an adequate period of time, in particular:
☐	Location of the sales/marketing department
☐	Job descriptions, liabilities and executive powers in the company during the relevant time and in the relevant area
☐	Data on money flaws through bank account inquires
☐	Information on sales agreements
☐	Compare those data with similar companies’ data (business analysis)
☐	Expanses recorded in the nominal ledger
☐	Performances of sales and marketing staff:

☐	To whom they have sent invitations?
☐	What kind of hotel bills, parking tickets, lunch receipts, fight tickets or bus tickets have been entered in the accounts? (this information can provide important insights about people involved)
☐	Cross checking the receipts with agents' and other suspects' receipts might provide good evidence
☐	Use of third party agents
☐	Has the agency-.relationship been registered?
☐	Where is the agent established?
☐	Where, how and how much has he been paid?
☐	How have those payments been recorded?

The Bribed: Public official	
☐	Public official income
☐	Wealth disclosure statement
☐	Job, income, wealth and other financial information about his family members
☐	Place of residence
☐	Activity of his office
☐	Family house ownership and acquisitions
☐	Cash flow analysis
☐	University tuition of familiars
☐	Vehicle ownership
☐	Travels
☐	Real estate ownership
☐	Employment of family members
☐	Academic tuition for family members

The investigators should be able to prioritize leads and information which may conduct to the development of a strong set of evidence against the offenders, for example:[97]

Personal residence

The personal residence ownership and acquisition transaction can reveal important information about the financial situation of the public official. A significant difference among the value of the purchase and the actual bank loan can reveal a very large initial payment at the time of purchase. Financial information relating to the purchase may be fairly easy to obtain in case the house had been purchased through a licensed Notary Public and the loan obtained at a major bank. The bank may maintain detailed records of the transaction, since they financed a significant amount and should have

conducted due diligence which may have included the source of the initial payment. The Notary Public may also have records of the complete transaction. In some economies, it is customary to use 'title companies' or 'closing agents' that act as an escrow agent or middleman to facilitate the purchase of the property between the buyer and seller. These entities also maintain complete records of all money flows between the buyers, sellers, taxing authorities and financial institutions. The seller of the property should also be interviewed to obtain the complete details of the transaction, including the method of payment for the house.

Cash flow analysis

If the public official maintains a bank account at a domestic financial institution, the records of this account should be requested very early in the investigation because it may require a significant amount of time for the bank to research the records. If the government salary of the public official has been deposited into this domestic account, it will be important to perform a complete analysis to establish how his legitimate salary has been spent. A cash flow analysis relating to any cash withdrawals or deposits should also be prepared. Once these financial flows have been analyzed, it will create a complete picture of the distribution of his legal funds and show how much cash was available for purchases. This may be very significant if expenditures are later identified from unknown or illegal funds. Large cash payments or purchases from unknown sources may be an important piece of evidence at trial.

University education

A common way to reward a corrupted official has proven to be the coverage of college and university tuition for sons and other relatives of the public official. Investigations into the public official's family members may reveal, for example, that his sons are attending prestigious university abroad and there is a very good chance that the official is not able to afford the corresponding tuition, living expenses and travel costs. In this case, investigators should try to determine whether or not a legitimate source of funding, such as a scholarships granted by the university, exists, and who is actually paying the university tuitions. The universities should therefore be contacted, the expenditures documented and the source of payments identified.

Vehicle ownership

Another major lead from the pre-investigation activities might be vehicle ownership of the public official or of his family members. For example, the fact that the public official's wife owns an expensive automobile is an indication that he may be living above his means. Investigation into the purchase of the vehicle purchase will involve first tracing the ownership of the car to determine the prior owner. This can lead to discover the records of the transaction, who was the purchaser, the date of the purchase, and – the most important – the source of the payment. If the payment were made by bank check, the dealership may have a copy of it. If the payment was made by cash, this is a an interesting piece of evidence, provided for example that the cash analysis of the public official's bank account has established that he did not had available a corresponding amount of cash from his legitimate sources of income.

B. Informants and suspects

For investigations into corruption cases, human intelligence resources are particularly invaluable in circumstances where there is a real lack of information about the corrupt network. In the case of serious economic offences and corruption, the individual who comes forward may well be a disgruntled former employee, a whistleblower, a company representative who has been cheated out of a procurement deal by large-scale bribery or even a former co-conspirator with an axe to grind.[98]

However, investigators must pay careful attention to the reliability of these sources of information, by considering the reasons and the motives for the individual wishing to pass on information and whether those motives might be malicious, and therefore misleading, with the potential to compromise the investigation, and whether any sort of inducement is sought for the information.[99] Investigators should therefore seek to corroborate the information provided by informants through other sources of evidence and investigative tools.

When dealing with informants and witnesses, a comprehensive interviewing strategy should be developed. The following areas should be addressed:[100]

Informants and witnesses	
☐	Provisions should be in place for the protection of witnesses. Witnesses' identity should remain confidential for as long as possible. Witness relocation or protection programs or a "new identity" program may be available. If the witness is in prison, provisions for a safe location in must be established. The appropriate policies need to be developed as soon as possible so as to be in place when the need arises.
☐	It is advisable to reduce opportunities for the defense lawyer to attack the credibility of the witnesses (by having recorded statements, transcribed and signed or initialed by the witness).
☐	Processes should be established to deal with lawyers who are either attached to the witnesses or to the potential defendants.
☐	If the witness has a criminal background, it is important that they be open about prior criminal activity (particularly if it involves the defendants) and to ensure sure that this information is disclosed to the court prior to the witness undergoing examination.
☐	Keeping witnesses informed of the criminal prosecution process will instill confidence in them and allay fear and apprehension.

Specific considerations are to be made with reference to the different categories of informant and to specific needs.[101]

Confidential informants

They are generally criminals. Unlike a cooperating witness, their personal information must be maintained as confidential. The motives of the informant may be revenge, financial gain, or personal protection (i.e., to avoid being sentenced to prison). It is important to note that confidential informants are almost never expected to testify in court.

Confidential sources

They are generally not criminals, but they provide information because of their position or employment. Attention must be given to safeguarding these sources' income in order to prevent it from being jeopardized due to interaction with investigators.

Cooperating witnesses

Cooperating witnesses supply their information in a confidential manner, but they are expected to become witnesses. Remember the importance of protecting witnesses. When using a source or witness, as described above, internal protocols and procedures need to be established as uniform policy. The following elements are important:

- ☐ Written agreements used to define the responsibilities of both the source and the law enforcement agency
- ☐ A system of either code words or names established that will be used in files to prevent accidental disclosure
- ☐ Original information kept separately from the general investigation files
- ☐ Limited access to the source files for those within the investigative agency
- ☐ Routinely audited financial records associated with source operations
- ☐ A third party present when payments are made to a source and receipts obtained
- ☐ Periodic reviews, at a managerial level, of the source files as an internal audit protection
- ☐ Any promises being made to the informant or witness cleared with the government agency or government attorney (It is good policy to have all promises in writing to protect the integrity of the investigator and the investigative process)

Protection of the Source/Witness

Threats to the source or witness should be anticipated before they actually occur, and the investigative team should be prepared to immediately respond. A threat assessment should always be performed for witnesses, and it must always be determined if the witness is fearful of an approach or an act against their person. There are two approaches to threats to witnesses:

- ☐ A reactive approach is the aggressive investigation of any threat or act of violence to a source. During this approach, no intimidation of any witness is tolerated

☐	A proactive approach involves having witness assistance and witness protection programs available. It is important to remember that most witnesses are frightened simply by being involved in a criminal process. These concerns need to be dealt with by the team

Table 22: *Physiological stressors*

SOURCE: D. D. DORRELL - G. A. GADAWSKI - H. BOWEN - J. F. HUNT, Financial Intelligence: People and Money Techniques to Prosecute Fraud, Corruption, and Earnings Manipulation, in *The United States Attorney Bulletin,* March 2012, v 60, n. 2.

For the purpose of extract information from people and to be able to read the signals hidden into the complex and dynamic nature of the people, law enforcement agencies should rely on a series of techniques and tools, which analyze physiological stressors in order to evaluate a personal statement or examination.

Those techniques rely on the assumption that s*tress typically results when subjects fabricate responses to questions*, and that learning how to detect physical signs of stress reaction can therefore help investigators to realize whether or not a person under interrogation is lying.

The US Department of Justice makes reference to a variety of technique and methods, designed to comprehensively evaluate the physiological indicators of stress.

- The CICO method (Concentric-In/Concentric-Out), a comprehensive investigation/cross-examination technique, which comprises virtually all indicators affecting a subject and permits the assessment of the integrity, probity, or veracity of a subject's behavior, and oral or written statements.
- Dr. Paul Ekman tools, like FACS, F.A.C.E, METT, and SETT, specifically intended to interpreting facial expressions (www.paulekman.com);
- Don Rabon interrogation techniques, which make use of questions focused on auditory, visual, and sensory memory and recollection, and that stress that eye movement prior to answering a question indicates fabrication depending on the direction of the movement (www.hamletsmind.com);
- The Reid Technique of Interviewing® and Interrogation, developed by John Reid, widely deployed as a means of structuring interrogation leading to confession (www.reid.com);
- Linguistic Style Analysis Techniques (LSAT), deployed by Loveland Colorado Police Department, which consists of parsing verbal content into structural components in order to compare and contrast the facts (linguisticstatementanalysis.com);
- The Wicklander-Zulawski company methods of interrogation, lie detection, behavior detection (www.w-z.com).

CHAPTER VI. THE GATHERING AND ANALYSIS OF FINANCIAL AND CORPORATE EVIDENCE

The success of any corruption or money laundering investigation depends largely upon the ability of the criminal investigator to track the ownership trail of money and other assets that leads away from the crime or the criminal activity.[102] In other words, the first step in the process of asset recovery is to trace the proceeds of crime –or assets subject to confiscation–. Integrated financial investigation is an essential element of any strategy targeting the proceeds of crime.[103] As noted in Chapter I of the First Part of this Handbook, a recognized best practice is to integrate the investigation team with forensic accountants and financial investigators.[104]

A. Tracing and Identifying Financial Assets

International standards today recognize financial investigations as one of the core elements of any law enforcement effort against corruption and the laundering of its proceeds.[105] A 'financial investigation' is defined as an enquiry into the financial affairs related to a criminal activity with a view to, inter alia, identifying and tracing the proceeds of crime or any other assets that are or may become subject to confiscation. It also includes an enquiry with a view to developing evidence that can be used in criminal proceedings.[106] As stated in the FATF Operational Issues Financial Investigations Guidance:

> *The major goal of a financial investigation is to identify and document the movement of money during the course of criminal activity. The link between the origins of the money, the beneficiaries, when the money is received and where it is stored or deposited can provide information about and proof of criminal activity.*[107]

Hence, the investigation of large-scale corruption cases should follow the money trail in order to establish links between the stolen assets and the proceeds-generating criminal conduct.

In complex financial crimes, the asset to be linked to the offence is more likely to be the product of an intervening transaction. As a result of the intervening transaction, the asset is in a fungible form, which makes it easy to exchange it for a different asset. Tracing the proceeds of crime is premised on the assumption that the criminal origin of assets can be concealed through transformation, and that transformed assets can

easily and speedily be moved between locations or across borders. The assets can be mingled with others and converted into other forms.

Table 23: Tools for rapid locating and freezing of assets and specialized asset recovery teams

SOURCE: Nine Key Principles of Effective Asset Recovery Adopted by the G20 Anticorruption Working Group, Cannes, 2011, available at:

http://StAR.worldbank.org/StAR/sites/StAR/files/asset_recovery_country_profiles.pdf

Principle 3 – Set up tools for rapid locating and freezing of assets. To facilitate the prompt identification of bank assets that may be proceeds of corruption, establishing tools that would allow competent authorities to obtain information from financial institutions in a timely fashion to determine whether an individual has access to banking facilities in that jurisdiction is critical. Such a search could be initiated upon appropriate domestic and international request. This could be achieved either through a central register of bank accounts that can be accessed by competent authorities or through a system which allows competent authorities to directly query all banks within a jurisdiction. The system should also enable competent authorities to rapidly freeze assets, whether through a temporary administrative freeze, automatic freeze upon the filing of charges or an arrest, or by order of an investigating magistrate or prosecutor.

G20 APEC Economies' practice:

Economy	**Practice**
Australia	-For identifying and locating bank accounts, a request has to be sent to all financial institutions upon court order decision. -For identifying real estate, there is local registration, but the beneficial owner is not disclosed in real estate transactions and such identity can be easily hidden behind legal structures. -For identifying companies, a registry exists. -There are no mechanisms in place to consistently and rapidly identify the holders of life insurance and securities.
Canada	-For all financial institutions in Canada, a court order must be obtained to identify and locate bank accounts. -For identifying real estate, landowners' registration/deed registration is conducted at the local (provincial) level as the regulation of property is provincial jurisdiction under the Canadian

	Constitution. -For identifying companies, registries exist at the national level and provincial levels for companies registered within those jurisdictions. Canada does not provide for shareholders' registries *per se*. Registries of securities holders are in place at the provincial level in Canada. -In addition, Canada has implemented measures under the Criminal Code's Proceeds of Crime provisions, the Proceeds of Crime (Money Laundering) & Terrorist Financing Act and the Controlled Drugs & Substances Act that allow Canada authorities to identify and trace assets.
Japan	-For identifying and locating bank accounts, a request has to be sent to all financial institutions by the Public Prosecutor or the Police. -For identifying real estate, landowners' registration/deed registration occurs at the local level, and the beneficial owner is not disclosed in real estate transactions and such identity can be easily hidden behind legal structures. -For identifying companies, companies maintain their own registries, and if Law Enforcement Authorities are refused access they must return with a court order. However a warrant can be issued within several hours by a judge and thus meets, in Japan's view, the requirement on the issue of the swiftness. -There are no mechanisms in place to consistently and rapidly identify the holders of life insurance and securities, excepting those held by trust companies and high-level public officials.
Republic of Korea	-For identifying and locating bank accounts, reliance is upon a request to be sent to all financial institutions by an authority upon court order decision. When analyzing suspicious transaction reports, the FIU has access to financial information without the need of a court order, but still needs to send a circulatory letter to all financial institutions in order to locate all the assets at stake. -For identifying real estate, the Land registration Department maintains a register of properties acquired by non-resident Koreans; otherwise, real estate agents hold the information. -For identifying companies, the Commercial Registration Office holds information on registration details at the national level, with additional details furnished to tax authorities, but broader company details are held at the company's registered office. -There are no central registry systems in place to consistently and

	rapidly identify the holders of life insurance and securities, and only those held by registered trust companies may be immediately accessible. Nonetheless, if an investigative agency has the court issued warrant, then the agency can obtain such information.
Mexico	-For identifying and locating bank accounts (of an individual or a company), a request has to be sent to all financial institutions by an authority (like the FIU for instance) with no need of a court order, allowing for location of assets by data matching undertaken by the financial institutions. However, the authorities are not allowed to request this information themselves, and must go through the relevant supervisory agency (National Banking and Securities Commission (CNBV), National Commission of Insurance and Bonds (CNSF), Tax Administration Service (SAT). When it is essential for verification of crime and responsibility of the subject under investigation, the request will be made by the Attorney General's Office (PGR) or the public servant who has been given the power or by the court (article 117 of the Credit Institutions Law). -For identifying real estate, the Land Registry [Catastro] is held by each of the federal States of Mexico. It is not computerized and therefore not easily accessible. -For identifying companies, a registry exists, but it is not clear that all States are linked into it, or even maintain their records digitally (SIEM: http://www.siem.gob.mx/siem/). -Any mechanisms in place to consistently and rapidly identify the holders of life insurance and securities in Mexico are unknown, and prosecutors should consult the following authorities: the Ministry of Finance (www.shcp.gob.mx), the Commission for the Protection and Defense of Financial Services Users (www.condusef.gob.mx) and/ or the National Commission of Insurance and Bonds (http://www.cnsf.gob.mx), in their respective jurisdictions.
United States	-For identifying and locating bank accounts under section 314(a) of the United States Patriot Act a request may be sent by the United States' FIU to all financial institutions, allowing for the identification and location of assets and transaction information by data matching undertaken by the financial institutions. -For identifying real estate, all real estate recording systems in the U.S. may be administered differently by each state, district or territory of the United States. Real estate records, including land ownership, are generally maintained at a county, borough, parish or municipal level and many, if not all, property records are available online and, if not, are otherwise publically available and

	"hand searchable." -There are no centralized ownership registries of publicly traded shares or non-banking financial interests such as life insurance holdings. -As for the ownership of securities, individual dealer-brokers have knowledge of the shares their clients hold and maintain such records. There are certain filings requirements under the U.S. Securities laws that would require the public disclosure of beneficial ownership interests for certain publicly traded companies and for certain stock ownership levels, but due to the heavily regulated nature of such companies, the US considers that they pose little risk of being secretly controlled by criminal elements.

Principle 6 – Create specialized asset recovery teams – a kleptocracy unit. Success is closely related to the existence of specialized team of investigators and prosecutors that focus on the recovery of assets, including on behalf of countries harmed by grand corruption (in some jurisdictions, an asset recovery office may fill this role). Such units should be properly resourced, have proper expertise and training, and have access to relevant databases, registries and financial information to allow practitioners to identify, locate, and freeze assets. They should also have authority to cooperate with foreign FIUs, law enforcement, and judicial authorities, and to provide technical assistance in "following the money" to third party countries.

G20 APEC Economies' practice:

Economy	**Practice**
Australia	The Criminal Assets Confiscation Taskforce (CACT) is a multi agency taskforce led by the Australian Federal Police (AFP) and includes the Australian Taxation Office and the Australian Crime Commission. The CACT was established to combat serious organised crime and is tasked with identifying and removing profits derived from criminal activity. The CACT works in partnership with the AFP Fraud and Anti Corruption Centre in order to identify, investigate and litigate appropriate asset confiscation matters at the Commonwealth level.
Canada	Canada does not have a single centralized unit for asset recovery. Canada employs a whole of government approach, which draws on the expertise of resources of multiple authorities including Canada's

	Central Authority at the Department of Justice, the Royal Canadian Mounted Police, the Department of Foreign Affairs and International Trade Canada to manage requests for asset recovery by foreign states. Canada has a comprehensive law enforcement regime for recovering assets related to domestic offences and for recovering proceeds in Canada derived from an act committed outside of Canada that, if committed in Canada, would have constituted an offence punishable by indictment in Canada. Thus, according to Canada, it has not been necessary to create a specialized central unit or team dedicated to asset recovery because the capacity to deal with such matters is integrated into existing resources.
Japan	While Japan does not have a specialized asset recovery team / kleptocracy unit, Japan's Government affirms that it has adequate mechanisms and is well able to identify assets, freeze or confiscate and return them in providing asset recovery assistance to requesting countries. Its effectiveness is guaranteed by a close cooperation among related governmental bodies.
Republic of Korea	In 2006, Korea has established a special team for AML Investigation and Recovery of Proceeds of Crime within the Supreme Public Prosecutors' Office which has seen analogues subsequently introduced to five district public prosecutors' offices as well.
Mexico	According to Mexico, the economy does not have a specialized unit exclusively dedicated to asset recovery. The various issues related to the subject, are the responsibility of different units within the Attorney General's Office (Procuraduría General de la República), such as: - The General Directorate of International Procedures, responsible for international legal assistance, based on international agreements and treaties signed by Mexico in the matter. It is also empowered to establish, in coordination with the competent authorities, communication channels and mechanisms of cooperation with foreign authorities and international organizations, for activities relating to asset recovery. - The Special Unit for Crimes Committed by Public Servants and Against the Administration of Justice of the Deputy Attorney Specialized Investigation of Federal Crimes. - The Special Unit Operations Research Illicit Resources and Currency Forgery or Alteration, responsible for monitoring the operations crimes illegal proceeds. - The General Coordination of Information and Financial Analysis (created in December 2012), to investigate the financial structures linked to alleged operations linked with criminal organizations and

	prevent the use of their resources to finance criminal activities.
United States	In 2010, the Department of Justice launched the Kleptocracy Asset Recovery Initiative and designated a core group of experienced prosecutors to work exclusively on recovering corrupt officials' criminal proceeds for the benefit of people harmed by theft. This initiative is led by the Asset Forfeiture and Money Laundering Section, Criminal Division, of the United States Department of Justice. This team also relies on experienced financial investigators from the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) and together with the Department of Justices' Office of International Affairs (OIA), Fraud Section, and other components, initiates investigations and helps trace, freeze, and recover the proceeds of corruption that may be located in or affect the United States.

When the assets are the proceeds of an offense, they will often be moved around the world using different schemes, such as off shore centers, corporate vehicles and a variety of financial transactions in an effort to launder the funds. Hence, investigators should be able to obtain information from financial institutions regarding financial transactions, pierce the corporate veil of a corporate vehicle to determine the ultimate beneficial owners and be capable of analyzing the obtained information.

1. Access to financial information

One of the most persuasive evidence in a corruption case is evidence that a person benefited financially from his allegedly corrupt activity. For example, evidence that the person deposited large sums of cash into a bank account, purchased expensive items with cash, or spent significantly more money than can be attributed to legitimate sources of income.[108]

To gather that kind of evidence (identifying the bank assets that may be proceeds of corruption and whether an individual has access to banking facilities), the competent authorities may need to obtain information from financial institutions. As Table 23 shows, some economies count with a central register of bank accounts that can be accessed by competent authorities, others have a system, which allows competent authorities to direct query all banks and other financial institution within a jurisdiction, and some need a court order to do it.

Financial institutions not only held information about the movements of a bank account, but also about direct debits, standing orders, credit and debit slips, supplemental

information such as managers' written notes, account opening forms, copy of identification used to open the accounts, safety deposit boxes, copies of ledgers of business, credit and charge card accounts, credit and charge card statements, pensions, insurance schemes, mortgages and even other previously unidentified accounts. All of this information, properly requested and, once obtained, analyzed, can show the lifestyle of individuals being investigated, their spending patterns, the payments to and from other persons and whether they are living beyond their legal income.

Financial information is usually crossed with databases and registers (i.e. registers of companies, data of stock exchanges), disclosure forms (asset disclosures, financial and tax statements by public officials and other persons) and available information about salaries, income and spending (bills, expense reports).[109] In a financial investigation, it is essential to conduct a thorough and combined analysis of these documents.

a. Use of open-source information

Evidence of corruption may be found through the analysis of publicly available financial information. The main source of such information is internet and the mass media. Publicly available databases, disclosure forms of public officials –which in many jurisdictions are publicly available-, disclosed corporate information, as well as news articles, represent valuable sources of information.[110]

Table 24: Best practices - Disclosure forms
In the United States, financial disclosure forms of public officials required by the Ethics in Government Act are useful tool in corruption cases. They provide prosecutors with information about gifts received, including by spouses and other relatives, travel, income and liabilities. Other disclosure forms, such as travel disclosure form, conflict of interest disclosure forms and lobbying disclosure forms are also elements of information and have constituted evidence in some corruption cases. Public information gathered by the US Federal Election Commission is also used as a source of financial information. In Australia, all Agency Heads and members of the Senior Executive Service (SES) in the Australian Public Service are required to complete a declaration of private and personal interests, in which income and asset disclosure is included. Furthermore, non SES employees who have responsibilities that require them to be particularly transparent about their private financial and personal interests may also be required to complete a declaration. The information included in the declaration can help

prosecutors to determine whether a person is living beyond his/her means and whether his/her wealth was legally acquired.

There are a great number of financial databases or sources of information about assets that are publicly available –whether for free or by paying a fee- and could be used by a prosecutor or investigator in a corruption case. The following box includes some of them available in APEC Economies.

Australian Securities and Investment Commission (www.asic.gov.au)
Maintains company and business name registers, containing information relating to companies such as registration status, officeholders and, in some cases, shareholders and financial statements.
Personal Property Securities Register (www.ppsr.gov.au)
It is a national online register where details of security interests in personal property can be registered and searched, at least by a creditor.
Financial Crimes Enforcement Network (FinCEN)
It is one of U.S. Treasury's primary agencies to oversee and implement policies to prevent and detect money laundering. FinCEN's work is concentrated on combining information reported under the Bank Secrecy Act with other government and public information. This information is then disclosed to FinCEN's customers in the law enforcement community.
Internal Revenue Service (IRS)
It is the U.S. government agency responsible for tax collection and tax law enforcement.
INTERPOL
Access to international network of criminal activity files, query by name or business name, request intelligence check to get complete file.
National Crime Information Center (NCIC) (FBI System)
The NCIC database currently consists of 21 files. There are seven property files containing records of stolen articles, boats, guns, license plates, parts, securities, and vehicles. There are 14 persons files, including: Supervised Release; National Sex Offender Registry; Foreign Fugitive; Immigration Violator; Missing Person; Protection Order; Unidentified Person; U.S. Secret Service Protective; Gang; Known or Appropriately Suspected Terrorist; Wanted Person; Identity Theft; Violent Person; and National Instant Criminal Background Check System (NICS) Denied Transaction. The system also contains images that can be associated with NCIC records to help agencies identify people and property items. The Interstate Identification Index, which contains automated criminal history record information, is accessible through the same network as NCIC. See details on the files.

National Law Enforcement Telecommunications System (NLETS)
It is the International Justice and Public Safety Information Sharing Network — a state-of-the-art secure information sharing system for state and local law enforcement agencies. It provides electronic messaging to allow information exchange between state, local, and federal agencies and support services to justice-related computer programs. Users include all U.S. states and territories, Federal agencies with a justice mission, and certain international agencies.
Treasury Enforcement Communications System (TECS II)
The U.S. Customs and Border Protection (CBP) agency operates the TECS system.[1] It is used by more than 20 federal agencies for border enforcement needs and the sharing of border enforcement and traveler entry/exit information. The primary mission of the system is to support the agency in the prevention of terrorist entry into the United States and the enforcement of U.S. laws related to trade and travel. The system processes over 2 million transactions daily.
U.S. Customs Service
Information on people and goods.
Financial Information Units
Can provide analytical research services, databases for evidence or leads to relationships between subjects and other persons or entities, link analysis to show connections, Suspicious Transaction Reports and many other financial information.
Electronic Data Gathering, Analysis, and Retrieval system (Edgar)
Financial disclosure documents that public companies are required to file with the SEC http://www.sec.gov/edgar/searchedgar/webusers.htm.
Audit Analytics (via WRDS)
Provides detailed audit information on over 1,200 accounting firms and 15,000 publicly registered companies.
Bankscope
Contains annual report data of both publicly listed and private banks worldwide.
BoardEx
Contains data from publicly listed companies about their board members.
China Stock Market & Accounting Research Database (CSMAR)
Is the comprehensive database for Chinese business research. CSMAR covers data on the Chinese stock market, financial statements and China Corporate Governance of Chinese Listed Firms.
Compustat global
Consists of annual and quarterly report data of listed companies, with an emphasis on

non-American and non-Canadian companies.
Compustat North America
Consists of annual and quarterly report data of listed American and Canadian companies.
Orbis
Financial data of 79 million companies worldwide.
Thomson One Banker (TOB)
Financial data from annual reports, as well as data about mergers and acquisitions and IPO's. Focus is on listed corporations, worldwide.
Worldscope
Financial information and annual reports of companies listed on the stock market all over the world.

b. Requesting financial information to financial institutions

Notwithstanding the importance of gathering information available through public opened sources, such information is usually only the basis for requesting access to information held by financial institutions. This information includes, but it is not limited to:

- bank accounts;
- all account-opening documentation, such as forms that identify the beneficial owner, partnership agreements, and copies of identity documents (not only accounts under the names of the targets, but also those accounts that list any of the targets as a power of attorney or a signatory);
- bank account statements;
- credit and charge card accounts information;
- credit and charge card statements;
- standing orders;
- documents related to account transactions, including client orders, deposit and withdrawal slips, credit and debit memos, and checks;
- wire transfer documentation;
- managers' written notes, client profile, any due diligence conducted by the financial institution, any other data probing the economic background of the client;
- safety deposit boxes information;

- copies of ledgers of business;
- pensions and insurance schemes;
- mortgages and loan documentation;
- other previously unidentified accounts;
- any reports of suspicious activity that were submitted by an employee of the financial institution;
- correspondence files maintained by the financial institution[111].

The information contained in these documents can show the lifestyle of a person, his/her spending patterns (i.e., their travels, meals, vacations, hobbies or other interests) and whether a person is living beyond their means or has any financial problem.

In addition, automated teller machines (ATM) can provide information on:

- Sums withdrawn;
- Geographical location at a certain time;
- Routines.[112]

In most jurisdictions, this information is considered protected by the right to privacy. Therefore, accessing to such information is subjected to specific standards of evidence showing that, prima facie, the information may be used as evidence in a criminal case.[113]

In addition to requesting production orders to access information held by the regulated sector or service providers, investigators may need to monitor the transactions of a specific financial product for a period of time. In such instances, some jurisdictions allow for the request to "account monitoring orders", which are *ex parte* orders issued by a court requiring a particular financial institution to provide transactional information for a specific period of time.

Moreover, investigators may use customer information orders which include[114]:

- The account number(s);
- The person's full name;
- Date of birth;
- Most recent address and any previous addresses;
- Date(s) of account opening and/or closing;
- Evidence of identity obtained by the financial institution for the purpose of money;

- Laundering regulations;
- Personal details (name, date of birth, addresses) of joint account holders;
- Account numbers of any other accounts to which the individual is signatory and details of the account holders.

Customer's information on companies may also be useful, including details such as the value added tax identification number (VAT number), registered offices and personal details of individual account signatories.

In some jurisdictions, *credit reference agencies* provide, or similar private agencies provide information on an individual's financial relationships and status. The information provided by these agencies includes:

- Financial history and credit status, repossessions;
- Names of financial associates;
- Address checking;
- Electoral roll data;
- Insurance information;
- Cars, purchases (hire purchase information);
- Properties;
- County court judgments;
- Telephone numbers and a list of all credit searches that have been carried out on a person including identity verifications;
- Relevant information on fraud linked to a particular address, and details on repossessions;
- Information on business proprietors (including cross-reference business registrations using address and telephone number data, and directors' names)[115].

Table 25: Legal Issues

SOURCE: StAR (Stolen Asset Recovery) Initiative, *Barriers to Asset Recovery*, 2011, pp. 58-59, available at: http://www.unodc.org/unodc/en/corruption/StAR.html.

Banking Secrecy Laws

Banks and other financial institutions in most jurisdictions are prohibited from divulging personal and account information about their customers except in certain situations mandated by law or regulation. Some jurisdictions deal with banking secrecy by giving prosecutors the ability to obtain information about the existence of an account but requiring that the prosecutor seek a judicial order to obtain additional information

about the contents and transactions of the account. In some jurisdictions, a bank cannot divulge any information to a prosecutor about a bank account without judicial approval. It may even be a serious offense to provide information about a bank customer to any third party, including domestic or foreign governments, unless very specific criteria are met. Investigators have few alternatives to obtain information about specific accounts holding stolen assets where strict banking secrecy laws are in place.

Banking secrecy laws can also prevent law enforcement agencies from sharing banking information and documents with their foreign counterparts, even where these agencies wish to assist the foreign jurisdiction. To overcome this obstacle, the information is sometimes provided without a formal MLA request. For example, FIUs can obtain information on an FIU-to-FIU basis, and membership in Egmont Group of Financial Intelligence Units helps facilitate this cooperation and expedites the exchange by offering members access to the Egmont secure Web site. Information provided in this manner, however, is often not admissible as evidence in court. This restriction can mean that the authorities know where the proceeds of corruption are located but are unable to prove it in court and therefore are unable to restrain, seize, or confiscate the assets.

As stated in the Legislative guide for the implementation of the UNCAC:

Bank secrecy rules have often been found to be a major hurdle in the investigation and prosecution of serious crimes with financial aspects. As a result, several initiatives have sought to establish the principle that bank secrecy cannot be used as grounds for refusing to implement certain provisions of international and bilateral agreements or refusing to provide mutual legal assistance to requesting States. The same applies to the Convention against Corruption, as we have seen above with respect to seizure and confiscation of proceeds of crime (art. 31, para. 7; see also para. 8 of art 46 (Mutual legal assistance)).

In cases of domestic criminal investigations of offences established in accordance with the UNCAC, State Parties are required to ensure that their legal system has appropriate mechanisms to overcome obstacles arising out of bank secrecy laws (Article 40). In accordance with Article 31, State Parties must – to the greatest extent possible under their domestic system – have the necessary legal framework to enable, inter alia, the empowerment of courts or other appropriate authorities to order that bank, financial or commercial records (such as real estate transactions, shipping lines, freight forwarders and insurers) be made available or seized. Bank secrecy should not be a legitimate reason for failure to comply.

Legal Privilege

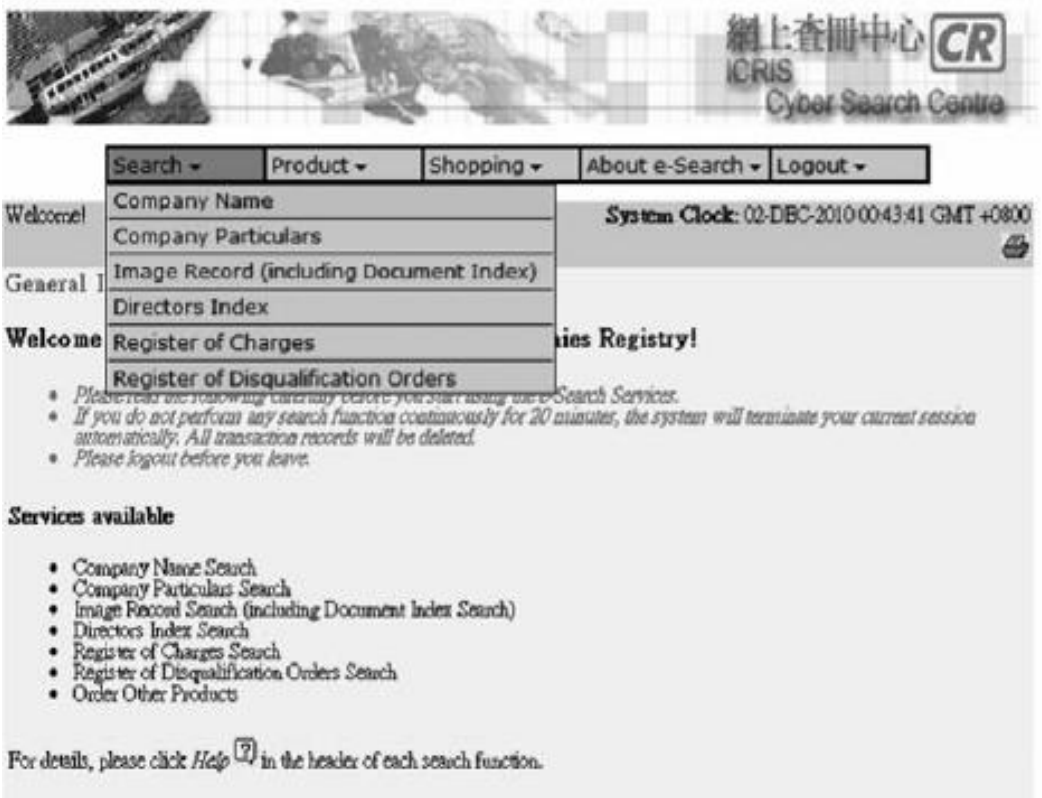
A barrier similar to bank secrecy laws may arise where claims of lawyer-client privilege prevent investigators from looking at transactions involving lawyers. Legal privilege is an important right and should be recognized in all jurisdictions. The privilege should not apply, however, in cases where the lawyer is providing financial services, rather than legal advice, or is acting as a financial intermediary.

2. Gathering information of corporate vehicles

The proceeds of an offense are usually hidden through the use of a corporate vehicle (companies, trusts, foundations, fictitious entities or unincorporated economic organizations) to disguise the criminal's role as the beneficial owner –the natural person who ultimately owns or controls the assets or the bank accounts of the corporate vehicle–.[116]

Table 26: Extensive Online Search Facilities Publicly Available at the ICRIS Cyber Search Centre in Hong Kong, China SAR

Source: StAR Initiative, *The Puppet Masters. How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do about It*, 2011, Figure 4.4, p. 79, available at: https://star.worldbank.org/star/sites/star/files/puppetmastersv1.pdf.



In those cases, the investigator will need to prove the link between the corporate vehicle and the beneficial owner. If the company is registered, the company registries are the entities that collect and store information on the structure and individuals that own and manage the entity.[117] This information includes: the name of the company,

legal entity type, the address of a registered office, the physical location or principal place of business, the names and addresses of a registered agent, person authorized to accept service of process, or a resident secretary, the names and addresses of persons in positions of legal control within the legal entity (directors and officers), and the names and addresses of persons in positions of legal ownership (shareholders or members).[118] One flaw of the information held by companies' registries is that sometimes it is not completely accurate or it is not kept up to date (quality assurance and updating are usually responsibilities of the legal entities).[119]

In recent years, many registries have begun to upgrade their systems to take advantage of recent developments in digitalization and electronic processing.[120] For example, the Integrated Companies Registry Information System of Hong Kong, China has created a Cyber Search Centre that permits investigators to access information about the entities on-line.

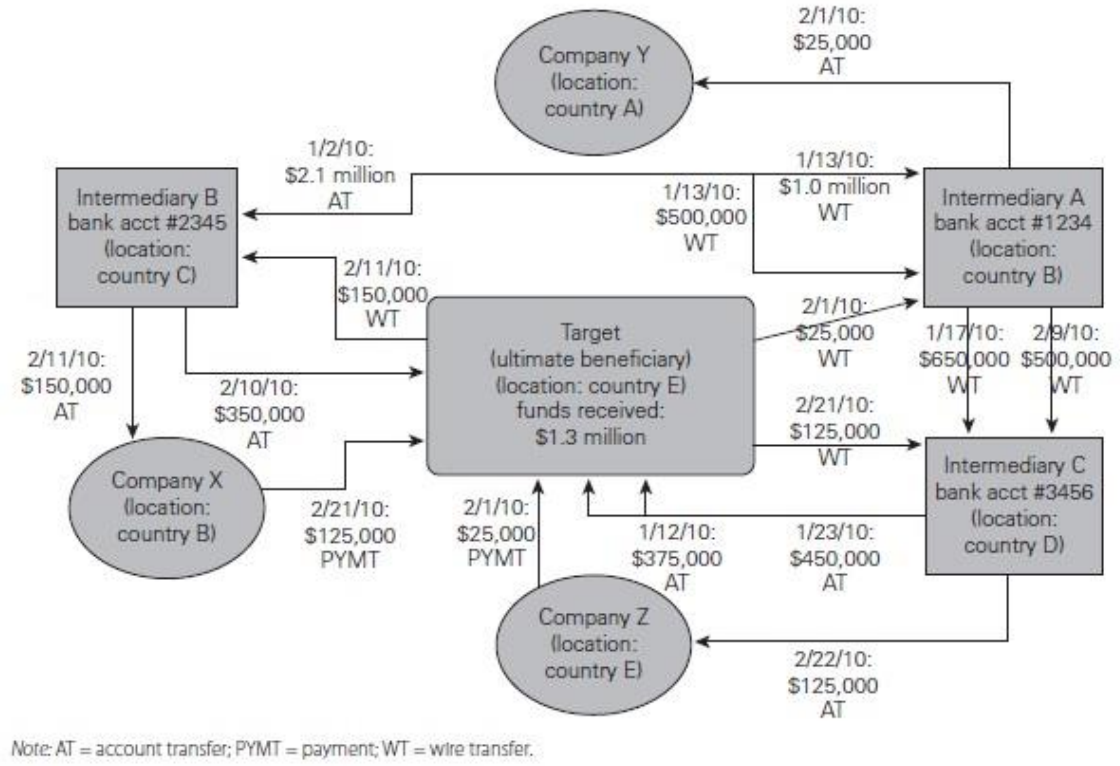
Furthermore, information regarding the name of the corporate vehicle, the documents incorporating the company, the names of the board members, and the names of the persons entitled to conduct business on behalf of the company are often held by service providers, among which are TCSPs and banks. These institutions are internationally obliged to conduct customer due diligence of the corporate vehicles to which they provide services.[121] However, some banks and TCSPs do not adequately identify the beneficial owner when establishing a business relationship, since, for example those in the United States, are not generally obliged to collect beneficial ownership information.[122]

Since the investigator will have to determine who ultimately effectively controls a corporate vehicle, it is useful to consider the type of corporate vehicle that is being analyzed:

Corporate vehicle	Persons having ultimate control
Companies	The shareholders, the board of directors, the executive officers.
Trusts	The trustee, the settlor, the beneficiary.
Foundations	The director or board, the private beneficiary

Table 27: Sample Flow Chart

SOURCE: StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 72.



This flow chart provide a visual snapshot of the target, associates, gatekeepers and corporations involved, as well as of the assets, bank accounts and corporate vehicles.

A typical obstacle to obtain information about corporate vehicles is that "the relevant documentation may be deliberately dispersed across different jurisdictions. Collecting information on a particular legal entity that is incorporated or formed under the laws of Country A but administered from Country B often entails first submitting a request to Country A and then submitting a request to Country B."[123]

Furthermore, if the company is an international business corporation (IBC), a structure typically used for shell companies (set up by nonresidents in off shore financial centers –OFCs-), obtaining information about them tends to be much more difficult since they usually have no economic activity and, if used illicitly, additional mechanisms are used to obscure the beneficial ownership, such as exercising control surreptitiously through contracts, adding layers of corporate vehicles to obscure the beneficial ownership, hiding behind bearer shares and ensuring that the beneficial owners are located in another jurisdiction.[124]

The challenge when investigating IBCs is to pierce the corporate veil and find the beneficial owner (the person who controls the company and its assets). In order to do this, investigators can ask information about the real owner to the jurisdiction where the company is registered. However, in offshore centers, the registry –where it exists-does not often require the actual identity of the beneficial owner.[125]

Table 28: The Case of Former President Augusto Pinochet (Chile)

SOURCE: StAR, *The Puppet Masters. How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do about It*, 2011, BOX 3.17, p.63.

Former Chilean president Augusto Pinochet funneled illicit proceeds through foreign corporate vehicles that named his family members and other close associates as the owners and controllers. For instance, Meritor Investments Ltd., Redwing Holdings, and a trust numbered MT-4964 were foreign corporate vehicles beneficially owned by Pinochet's son, Marco Antonio Pinochet Hiriarte and his daughter Ines Lucia Pinochet. Bank accounts were also opened under the names of these two persons, as well as another daughter of Pinochet, Maria Veronica Pinochet. Oscar Custodio Aitken Lavancy, an attorney who had ties to Pinochet, controlled six other corporate vehicles involved in the scheme. Pinochet's family members and Aitken effectively served as front men for Pinochet, allowing him to disassociate his name from the scheme while maintaining control over the assets.

A recent study by the StAR Initiative has surveyed around 40 jurisdictions, including most off shore centers located in the Caribbean and Europe, about what information is registered in the company registry, whether there is a residency requirement, whether bearer shares are still allowed and whether corporate directors or nominee directors are permitted.[126] Table 29, below excerpts those features for selected APEC Economies:

Table 29: An Overview of Corporate Vehicles in some APEC Economies

SOURCE: Extract from StAR Initiative, *The Puppet Masters. How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do about It*, 2011, Table E.1, pp. 220-231, available at: https://star.worldbank.org/star/sites/star/files/puppetmastersv1.pdf.

Economy	Information registered	Is there a residency requirement?	Bearer shares permitted?	Corporate directors permitted?	Nominee directors permitted?	Foreign companies registered	References

Delaware, United States	Registered office Registered agent	No	No	No	✓	✓	Delaware Code, Title 8, Ch.1, §§101, 132, 141(a), 145, 158, 371
Florida, US	Physical address Registered office Registered agent Managers/directors Officers	No	No	No	✓	✓	Florida Business Corp. Act, §607 (203, 723, 802, 850, 1401, 1501, 1503); OECD Tax Co-operation 2009, "Towards a Level Playing Field," p.122
Hong Kong, China	Registered office Managers directors Legal owners Officers	Company secretary must be resident	No (Warrants permitted)	✓	✓	✓	Hong Kong Companies Ordinance, §§14, 73, 153(B), 154, 333
Nevada, United States	Registered office Registered agent Managers/directors	No	No	No	✓	-	Nevada Revised Statutes, §§78.030, 78.035, 78.235(1), 78.115, 77.310
Ontario, Canada	Registered office Managers/directors	No	Dematerialized	No	✓	-	Business Corporations Act, §§5, 14, 100, 118, 119, 136; Securities Transfer Act 2006
Singapore	Physical address Registered office	At least one director must	No, unless issued before 29 Dec 1967.	No	All directors under the Companies	✓	Companies Act, Ch. 50, §§19, 66,

	Managers/directors Officers	be ordinarily resident	Current s66(2) of the Companies Act provides that bearers of share warrants issued before that date are entitled, on surrendering them for cancellation, to have their names entered into the company's register of members. However, a new transitional provision in the Companies Amendment Act will provide that the bearers of such share warrants shall within 2 years after the commencement of the Act be entitled, on surrendering them for cancellation, to have their names entered into the company's register of members. The company shall cancel any share warrant unaccounted for by the expiry of the 2-year period.		Act, by whatever name called, will have to comply with the legal obligations imposed on directors in the Act.		126, 142, 143, 145, 171, and 173.
Wyoming, United States	Registered office Registered agent	No	No	No	✓	✓	Wyoming Business Corporation Act, §17-16-201, -202, -625, -723, -802, -803, -851, -1801; §17-17- 102

Consequently, in gathering information of corporate vehicles, investigators have access to publicly available information, law enforcement databases, information held by entities such as financial intermediaries (banks and other financial institutions) and TCSPs, companies' registries, among others. Investigators also count with useful tools such as their compulsory powers (subpoena powers, search and seizure) and mutual legal assistance.

However, investigators usually encounter obstacles identifying the beneficial owners of involved corporate vehicles due to different factors. On the one hand, because of the lack of availability of beneficial ownership information in a given jurisdiction since, for example, it is not require by the corporate registry or a corporate service provider, or because of stringent bank secrecy or other anonymity laws that impeded their access to beneficial ownership information held by some institutions. On the other hand, due to the type of corporate vehicles, such as IBCs (which are not required to have a physical presence in the jurisdiction of their formation) or Limited Liability Corporations (whose simple structures allow for formation with as few as one member). Bearer shares, layering and multiple jurisdictions, as well as the lack of harmonization of international standards regarding covered entities under domestic AML regimes are other challenging obstacles to overcome.[127]

The investigators that integrated the StAR Initiative project made a number of recommendations to overcome those obstacles such as the adherence to a more flexible definition of beneficial owner, increasing information-sharing among domestic law enforcement and regulatory agencies, extending greater international assistance, including considering taking non-coercive measures even when the criterion of dual criminality is not fulfilled, building the investigatory capacity needed to take on the increasingly complex corporate vehicle misuse investigations and harmonizing international standards.[128]

B. Analyzing Financial Evidence

After tracing and identifying the assets, the analysis of the evidence is the next step to prove the illegal trail of the assets.

There are different types of methods for proving the receipt of unlawful income that an investigator or prosecutor of the APEC economies could use in a corruption case. The type of evidence available will dictate which method is most appropriate for a particular case. These methods could be direct, such as the *specific item method*, or indirect,

such as the *net worth method* or the "source and application of funds method". We refer to some of these methods below:

Specific Items Method
The specific item method is used when there is evidence that can directly trace the flow of money from the corrupt activity to the official. For example, when the prosecutor or investigator has a witness who can testify that he carried bribes to a public official on behalf of a third party or paid the bribes directly to the official on behalf of himself, this evidence constitute a "specific item" proof that will support a corruption charge. Or when a bribe was paid sending a wire transfer from the company's bank account directly to the bank account of the public official. This type of evidence is often used together with an indirect method of proof (whether a net worth method or the Source and Application of Funds method) which uses circumstantial evidence to support a corruption charge.
Net Worth Method
The net worth method is an organized process by a Law Enforcement Agency in which intelligence is gathered to determine if public officials are living significantly above their legitimate means. The project is not an initiation of criminal proceedings; it is merely the collection of public and government database material and other non-public law enforcement information relating to a group of public officials, such as all persons at or above Deputy Minister level or all procurement officers. This data is used to make a comparison of total assets owned by a person relative to their tax returns and asset declaration statements. If the computation discloses a significant increase in the net value (excluding appreciation) of assets that is many times more the known and legal income of the official, then the possibility of corruption may have been detected. Additional information will be needed to further support this suspicion.[129] The net worth method is often used in situations where an individual invests illicit gains in property such as stocks, real estate and business ventures. The investigator will have to prove that the suspect has underreported income (i.e., there are discrepancies between an individual's income for a given period and their net worth). First, it will have to be established the person's opening net worth or total net assets at the beginning of the period that is being investigated. Next, the investigator will have to present evidence of the increase in the suspect's net worth over the investigated period. The

source of this increase has to be a taxable one, such as the receipt of bribes. The evidence could also include the lack of nontaxable sources of funds in the investigated period that could account for the increase in net worth (gifts, inheritances, loans, etc.). Finally, the unreported income that represents the bribe or the unlawfully-derived income will be the difference between the reported income of the suspect and the increase in net worth for that period.

The Source and Application of Funds Method

The Source and Application of Funds method of proving the amount of illegal income is used when direct evidence is not available and the investigation discloses that the subject spent far more money during a set period of time than he had legally available to him. This set period of time can be any amount of time that demonstrates an increase in spending or wealth far above the legal means of the subject.[130]

The basic theory for this method is that the person under investigation spent far more money during a set period of time than he had legally available to him.[131]

For example:

> For the set period 1 January 2012 to 31 December 2012 the defendant had:
>
> Total expenditures and other applications of money USD 50,000,000
>
> Total of known and legal sources of income USD 2,000,000
>
> Equals illegal or unexplained income USD 48,000,000

The total and cash expenditure methods are the most useful methods of financial proof in a corruption case. These methods are usually employed in typical corruption cases where the person spends the unlawfully-obtained cash on consumable items (food, entertainment, clothing, travel, or other items that are not traceable, such as cashier's checks, money orders, traveler's check, etc.).

In the total expenditure method, the prosecutor or investigator should calculate a "starting point," reflecting how much cash the suspect had at the beginning of the investigated period, through financial statements, loan applications, financing arrangements, economic disclosures statements, admissions made to investigators, or a review of their financial condition prior to the charging period. And then, the person's expenditures for the given period should be totaled – the investigator or prosecutor should look for increases in cash deposited into the suspect's bank accounts, cash purchases, checks written, third-party checks issued to the suspect, personal

expenditures, etc. –. If those expenditures exceed his reported income for the investigated period of time and the available cash at the beginning of that period, the excess represents the amount of unreported unlawfully-obtained income that constitutes the basis of the investigated criminal conduct.

The cash expenditures method deals solely with the suspect's use of cash, which include withdrawing cash from a bank account, receiving cash loans, writing checks for cash, cashing salary or third-party checks, etc. By calculating all of the person's cash expenditures and subtracting all legitimate cash sources, the prosecutor can conclude the amount of cash expenditures that exceeds the legitimate sources of cash for the investigated period, which represents the cash bribes, payoffs, or otherwise illegally-obtained funds resulting from the suspect's corrupt conduct.

It is often used to create a prima facie case that the individual is corrupt. The investigator or prosecutor has to establish the disproportionate income, property, or assets. When material possessions are of an amount or value so disproportionate to the person's official or other earnings, the burden of proof shifts to the suspect who will have to prove the lawfulness of the sources from which he have acquired those possessions.

It must be proved that the suspect maintained a standard of living not commensurate with present or past reported salary, or with benefits, during the investigated period.

Special attention should be paid to the fact that the suspect's relatives of friends might be the ones in charge of the control of the property or assets on the suspect's behalf.

In summary, it is necessary to prove the disproportion among the property, the amount of monetary resources or assets that were controlled by the suspect's during the investigated period, and the total payments made up to during the same period. Additionally, all outgoing payments and capital accretions, both domestic and abroad, should be analyzed, which includes:

- Goods and services acquired during the investigated period;
- Running costs, expenses of repairs, or maintenance and outgoings, incurred during that period (and/or connected with the property acquired before that date);
- The value of any gifts given;
- The money spent by the suspect on another individual;
- The ability to obtain credit during the given period;

- The value of services obtained on credit;
- Prepayments that were made during that period;
- Amount of salaries or hires paid during the period;
- Bills remaining unpaid for goods and services rendered during the period;
- Increase in the defendant's bank account between the beginning and end of the period being investigated;
- Deposits and investment made by or for the defendant, family, etc.;
- Payments made by third parties for the benefit of the defendant;
- Credit given for money received from sale of assets or goods before the charged period (if shown they come from an untainted source); and
- All sources of income.[132]

Furthermore, he suspect might also have accounts at banks separate from those where legitimate sources of income are deposited; hence, the prosecutor or investigator should require the suspect's bank information from all the financial institutions in the areas where the person lives, works or has any connection, such as a vacation home.[133]

1. Analyzing bank records

The analysis of bank records is an essential task in a financial investigation. Although it could be seen as a complex and difficult task, even nonfinancial experts are able to conduct some initial analysis. Table 30 summarizes those initial steps:

Table 30: The analysis of bank records

SOURCE: ATKINSON P., “Asset tracing”, in *Emerging trends in Asset Recovery*, p. 230.

The first step is to organize the records in an electronic database (i.e. an Excel spreadsheet). Once all data from the bank account has been entered into the spreadsheet, either manually or by a computer process, the analysis will be divided into three relatively easy tasks, namely the analysis of the deposits, the analysis of the disbursements and the identification of balances on certain dates.

The deposit analysis will include reviewing each item deposited into the account and determining its source: legal, illegal or unknown. For some deposits, such as salary payments, their type (legal, illegal or unknown) may be easily determined by simply reviewing the bank documents. However, if the source is unknown, the investigator will have to make third party contacts to inquire about the purpose of the payment that was made to the subject. By developing a list that summarizes and totals each type of deposit, the investigator can focus on what leads are most important to follow.

The analysis of the disbursements can be accomplished in the same manner. The investigator can now quickly identify which items require additional follow-up or detective work. This disbursement analysis assists in identifying assets purchased, business associates, transfers to other bank accounts, international money movements and spending that exceeds the subject’s legal income.

In some cases, it may be important to identify the balance that is in the bank account on a particular date or on a series of dates. This also can be quickly accomplished by adding a column in the Excel spreadsheet that automatically calculates the balance following every transaction.

These are the three basic types of analysis that should be completed for each bank account. In addition, there are other records maintained by banks that should be reviewed, such as account opening documents, bank due diligence reports, loan files, electronic funds transfers and correspondence files.

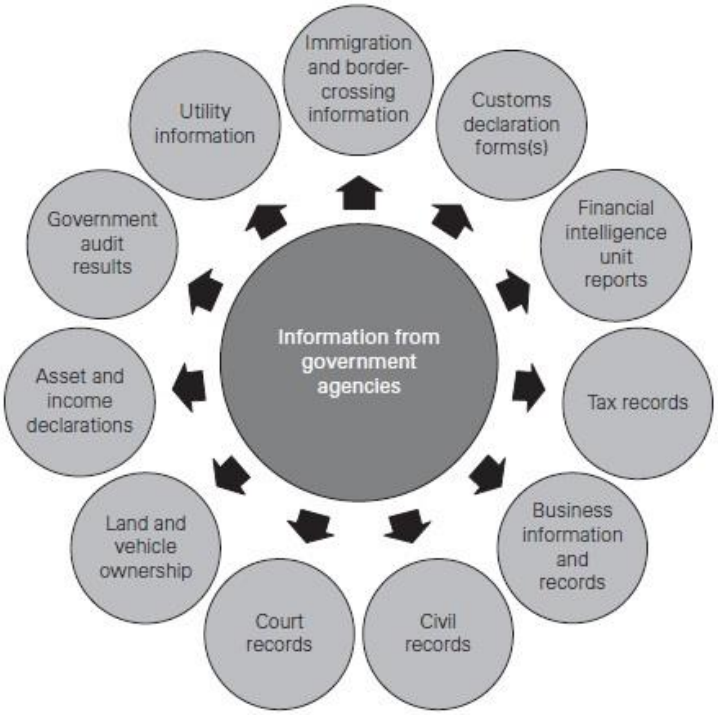
C. Obtaining Assistance from another Economy

In the process of asset tracing, it is often the case that crucial information is located in another jurisdiction. Therefore, obtaining assistance from another economy is crucial for the success of the financial investigation. The figure included below shows the preliminary information available from other economies’ agencies:

Table 31: Information from government agencies

SOURCE: Source: StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 49, Figure 3.2, available at:

https://StAR.worldbank.org/StAR/sites/StAR/files/Asset%20Recovery%20Handbook.pdf.



Most APEC Economies have ratified the UNCAC,[134] which serves as a basis for legal mutual assistance in the investigation of corruption offences. In addition, several MLA treaties and domestic legislation of the APEC Member economies expressly require the economy to trace and identify proceeds of crime in their jurisdiction upon request from another member. Often, the tracing and identification of assets do not involve any special MLA procedures but only the gathering of documents. However, some APEC economies have additional measures designed specifically for the tracing of proceeds of crime. For example, Australia's MLA legislation allows courts to issue production orders for "property-tracking documents". These orders compel persons (e.g. financial institutions) to produce documents relevant to the identification, location or qualification of proceeds of a serious foreign offense. The legislation in Papua New Guinea contains similar provisions.[135]

Another tool to trace proceeds of corruption is the monitoring of an account at a financial institution. At the request of another economy, Australia may seek a monitoring order from a court. Such an order compels a financial institution to provide

information about transactions conducted through a specific account during a particular period of time. However, these orders are only available if the investigation pertains to a crime punishable by at least three years imprisonment.[136]

Information regarding the assistance that some of the APEC economies provide to foreign authorities and how they provide it is included in the table below:

Table 32: Mutual Legal Assistance – Selected APEC Economies

Australia	The International Crime Cooperation Central Authority within the Attorney-General's Department Australia is designated as the central authority for extradition and mutual assistance matters generally. The Central Authority's contact information, and steps to follow when seeking mutual legal assistance from Australia, can be found in the step-by-step guide 'Requesting Mutual Legal Assistance in criminal matters from APEC economies' at http://publications.apec.org/publication-detail.php?pub_id=1608. An overview of the mutual assistance process is also available at http://www.ag.gov.au/Internationalrelations/ Internationalcrimecooperationarrangements/MutualAssistance/Pages/default.aspx. Australia has designated appropriate authorities responsible for mutual legal assistance requests relating to asset recovery as well as points of contact for law enforcement cooperation with UNODC (UNCAC asset recovery focal point). Australia participates in the Global Focal Point Initiative supported by STAR/INTERPOL.
Canada	The Canadian Central Authority (International Assistance Group, Department of Justice Canada) for handling MLA provides information on the MLA process which can be accessed at http://www.justice.gc.ca/eng/cj-jp/emla-eej/mlatocan-ejaucan.html. Further, according to Canada's AR Guide, its MLA process is described in the "G8 Step-by-Step Guide on Mutual Legal Assistance," at http://www.coe.int/t/dghl/standardsetting/pc-oc/PCOC_documents/8_MLA%20step-by-step_CN152011_CRP.6_eV1182196.pdf. The 2012 G20 "Requesting Mutual Legal Assistance in Criminal Matters from G20 Countries: A Step-by-Step Guide" (2012) also describes Canada's MLA process. Canada's Asset Recovery Guide indicated that the description of Canada's MLA process is available in French and Arabic through the Canadian Central Authority. The contact information is given on page 9 of the Asset Recovery Guide. Canada liaison office in Brussels to facilitate processing of MLA requests from countries in Europe and liaison official in Paris to assist in the processing of

	requests to and from France. Informal assistance may be provided by the FINTRAC (FIU and FI Supervisor) http://www.fintrac.gc.ca/, the Office of the Superintendent of Financial Institutions http://www.infosource.gc.ca/inst/sif/fed04-eng.asp, provincial securities regulators, and the police. MOUs are required only by FINTRAC (both as supervisor and as FIU). All other authorities are empowered to provide certain decentralized types of assistance in the absence of MOUs. The Royal Canadian Mounted Police has a network of liaison officers posted in strategic locations around the world. The aim is to support the RCMP's mandate in the fight against transnational crime by training and deploying highly skilled multilingual officers to those various strategic locations. In addition to international operational support, the network of LO also enhances and supports the GoC's commitment for mutual cooperation and the need for Canada to maintain, enrich and develop partnerships throughout the world. Canada has designated appropriate authorities responsible for mutual legal assistance requests relating to asset recovery as well as points of contact for law enforcement cooperation with UNODC (UNCAC asset recovery focal point). Canada participates in the Global Focal Point Initiative supported by StAR/INTERPOL.
Japan	Japan facilitates smooth process of asset recovery and enhances multilateral network among organizations for asset recovery by joining Asset Recovery Inter-Agency Network in Asia and Pacific (ARIN-AP) as a core member and Arab Forum on Asset Recovery (AFAR). Japan has been enhancing bilateral network for asset recovery by increasing the number of Mutual Legal Assistance Treaties (MLAT) and Mutual Legal Assistance Agreements (MLAA), which covers around 80% of the MLA requests Japan received in 2013, up from around 40% in 2008.
Republic of Korea	Korea's Central Authority for MLA is the International Criminal Affairs Division, Criminal Affairs Bureau, Ministry of Justice. In December 2012, the Korean Supreme Prosecutors Office hosted a meeting in Seoul with other Asia Pacific countries to establish the Asset Recovery Inter-Agency Network for Asia and the Pacific (ARIN-AP). Korea offered to house the ARIN-AP secretariat, establish a website in January 2013 and then to organize a meeting in first quarter of 2013 to solicit input by other countries. Korea has designated appropriate authorities responsible for mutual legal assistance requests relating to asset recovery as well as points of contact for law enforcement cooperation with UNODC (UNCAC asset recovery focal point). Korea participates in the Global Focal Point Initiative supported by StAR/INTERPOL.
Mexico	While Mexico provides a good deal of information online on the mechanics of informal and formal cooperation process (Information on letters rogatory: http://www.sre.gob.mx/english; Tracking service for letters rogatory: http://webapps.sre.gob.mx/rogatorias/; Attorney-General's Office- requests and

	receives MLA requests on criminal matters: http://www.pgr.gob.mx/; Assistant Attorney General for Special Investigations and Organized Crime: http://www.pgr.gob.mx/prensa/2007/coms07/170407.shtm; Financial intelligence unit: http://www.apartados.hacienda.gob.mx/uif/index.html), the extent to which cooperation regarding asset recovery takes place in practice is not known. Mexico has designated appropriate authorities responsible for mutual legal assistance requests relating to asset recovery as well as points of contact for law enforcement cooperation with UNODC (UNCAC asset recovery focal point). Mexico participates in the Global Focal Point Initiative supported by StAR/INTERPOL.
United States	The US Central Authority for MLA is the Office of International Affairs of the Criminal Division of the Department of Justice (OIA). The US provides resource personnel or liaisons to assist with international cooperation. This includes OIA attorneys who are assigned to work with specific countries, other DOJ subject matter experts, as well as DOJ attachés and law enforcement attachés who are posted to numerous U.S. embassies abroad. The United States has designated appropriate authorities responsible for mutual legal assistance requests relating to asset recovery as well as points of contact for law enforcement cooperation with UNODC (UNCAC asset recovery focal point). United participates in the Global Focal Point Initiative supported by StAR/INTERPOL.

In some jurisdictions, disclosure obligations is a barrier to MLA requests since it obliges authorities to provide notice to the targets of those MLA request, granting the targets the right to appeal a decision to provide the assistance. This requirement implies a risk for the financial investigation; it could lead to the dissipation of funds and to lengthy delay (the target will try to block the process and use all legal barriers at his/her disposal to exhaust all instances of appeal).[137]

Some proposals to circumvent this barrier are:

- "Discuss issues and strategy with foreign counterparts;
- Consider conducting a joint investigation or providing information to the foreign authorities so that they can conduct their own investigation and take provisional measures. Either option may remove this potential avenue for delay because disclosure to a target can be postponed for domestic investigation and provisional measures;
- Ensure that a request is not overly broad to prevent potential arguments that the request breaches privacy;

- Ensure that facts and reasons for the request are outlined clearly to address potential arguments that the dual criminality test is not met—that is, a target may argue that the request is a tax investigation colored as a corruption investigation and intended to go around the dual criminality principle."[138]

Table 33: Facilitating Informal Assistance

SOURCE: StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 134, Box 7.5.

Informal assistance is generally conducted on a counterpart-to-counterpart basis, a process that introduces a middleman in some exchanges because law enforcement must go through its domestic financial intelligence unit (FIU) to obtain information from an FIU in a foreign jurisdiction.

Some jurisdictions have moved to facilitate informal exchanges by permitting direct cooperation, regardless of whether the foreign agency is a counterpart. For example, the U.S. Financial Crimes Enforcement Network cooperates directly with foreign law enforcement agencies from the European Union in certain circumstances, and similar cooperation is reciprocated.

Table 34: National institutional frameworks

SOURCE: Nine Key Principles of Effective Asset Recovery Adopted by the G20 Anticorruption Working Group, Cannes, 2011.

Principle 7 – Actively participate into international cooperation networks. National institutional frameworks should be set up to ensure that foreign authorities are able to obtain all relevant information on the proceeds of corruption in a timely manner and to enable prompt legal action in response to foreign requests. Such institutional framework include:

a. Establishing focal points of contact for law enforcement and clear and effective channels for mutual legal assistance requests related to corruption and asset recovery.

b. Working with existing networks (policy or operational), such as UNCAC, Interpol/StAR, the International Corruption Hunters Alliance, CARIN, and the

meeting of law enforcement authorities at the OCDE, amongst others to identify possible gaps and best course of action in multi-countries international investigations and prosecutions.

c. Encourage informal contacts with foreign counterparts particularly before the presentation of mutual legal assistance requests.

d. Make information publicly available on what assistance does or does not require an official MLA request and applicable procedures and legal requirements for pre-MLA and MLA international cooperation (including whether UNCAC is a sufficient basis for MLA).

e. Encourage spontaneous disclosures by domestic authorities, a proactive form of assistance which alerts a foreign jurisdiction to an ongoing investigation in the disclosing jurisdiction and indicates that existing evidence could be of interest.

f. Improve capacity to respond to MLA request in grand corruption cases. Granting mutual legal assistance even in cases of minor technical or formal deficiencies should be the norm. Allocating increased staff and resources to work with the foreign jurisdiction in the drafting or clarification of requests will help to avoid such deficiencies.

CHAPTER VII. RESTRAINING MEASURES

Asset tracing is a time-consuming and resource-intensive effort of little value if no asset is available for confiscation in the end. For this reason, it is crucial that restraining measures be taken early on to secure the assets that may become subject to a confiscation judgment.[139]

Freezing and seizure mechanisms can be swiftly applied in order to preserve assets subject to confiscation and prevent their removal. Freezing orders are a form of mandatory injunction issued by a judge or a court that restrains any person from dealing with or disposing of the assets named in the order, pending the determination of confiscation proceedings. Freezing orders usually require judicial authorization (though some jurisdictions allow for orders by prosecutors or other authorities), and they do not result in the physical possession of the asset. Seizure orders, by contrast, involve the taking of physical possession of the targeted asset. They also generally require a court order or, in some jurisdictions, they can be issued by law enforcement agencies. The applicable standard to determine the assets subject to these measures is the reasonable suspicion or belief that the assets are the proceeds or an instrumentality of crime.[140]

A. Strategic considerations before applying for a restraining measure

Before applying for a freezing or seizure order, investigators needs to consider several issues. First, the timing for applying to an order is essential to the success of freezing and seizure orders. If measures are imposed “too early”, the target may be tipped off and cease activities (thereby making it difficult to gather evidence and identify other accounts, targets, or the typologies used). By contrast, if the measures are imposed after a target is aware of the investigation, assets will likely be dissipated or hidden. For these reasons, criminal investigators and asset tracers should work together from the early stages of any investigation and certainly before any overt action is taken against a target in order to develop a strategy that will permit criminal investigation objectives to be achieved together with the restraint or seizure of a target’s assets at the optimal time. Such uncertainty may be overcome by monitoring the identified assets and, at the same time, alerting the target –e.g., through a summon, a subpoena, a hearing, calling a witness that will tip the target off, etc.- without letting him/her know that some of his/her assets are being monitored. This way, subsequent asset movements can be

traced. This strategy needs of course to be pursued with strict compliance of due process rules and defense rights, which varies in each Economy.

Usually, a target will be tipped off at the time they are charged with a criminal offense. They can also become aware in the course of an investigation when certain techniques are used (search of residences or businesses, interviewing witnesses, production orders, or issuance of a MLA request). It will be important to ensure that assets are secured before (or simultaneously with) the use of these investigative techniques.[141]

Two opposing principles must be balanced when provisional measures are applied. The first one is the public interest in ensuring that the proceeds and instrumentalities of crime are preserved and maintained until the end of the confiscation case, and the second is the right of the individual to enjoy the ownership and use of their property.[142] Often, targets have complicated holdings that involve third parties with legitimate interests (business partners, investors) and others whose interests' legitimacy may be questionable (owners of an asset controlled by the target, *mala fide* purchasers).[143] It is expected that provisional measures will be strongly contested or appealed by targets as well as third parties, especially when substantial property interests are subject to restraint or seizure. However, the application process for provisional measures must not be turned into a mini-trial in which allegations supporting the application are challenged. As provisional measures simply require a reasonable belief of certain *prima facie* facts, prosecutors should urge the court to avoid deliberating on the merits of the case, which will be most appropriately determined at trial by the court dealing with the related confiscation process.[144]

Freezing proceedings should respect *bona fide* third party interests as far as possible: "practitioners should be open to submissions from third parties in all cases and, where permitted, should consent to vary the restraint order or release assets or instrumentalities held legitimately. However, where no satisfactory or verifiable explanations can be given or there is a compelling public interest to seize the asset (for example, a drug house), third-party claims should be left to the court to determine in accordance with the criteria set out in the legislation for the protection or exclusion of third-party interests from restraint and confiscation".[145]

Table 35: Adapting the scope of a restraining measure to respect legitimate third party interests

SOURCE: StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 87-88

• Businesses and investment ventures: Practitioners must ensure that interests held by third parties in businesses and investment ventures are bona fide, and not beneficially owned or controlled by a target. If confirmed, the order must be drafted in such a way that the third party's interest are not restrained or seized. One way to do this is to require in the order that the business continue operating normally, but with strict reporting requirements to the court and oversight by the asset manager. This way, uninvolved third parties can participate in and benefit from the business, while the target is excluded from its management and does not receive any benefits.

• Assets jointly owned by a target and an innocent third party: When property is co-owned by the target and a third party who has used legitimate funds to purchase it and was not complicit in any way with the illegal activity, it may not be appropriate to obtain a restraint order over the entire asset. Instead, the order can be directed to restraining "the interest of [the target] in [a specific asset]". In practice it will be difficult for the third party to deal independently with an asset under this order; despite this, it will help to clarify that a future confiscation order will not apply to the third party's interest in the property.

• Liens and securities: Often, a lien or security held by a person or entity that had no involvement in or knowledge of the illegal use of the asset will apply to the property (e.g., a loan issued by a bank). Some jurisdictions have streamlined a process for recognizing such creditors as innocent holders where satisfied that they were in no way complicit in the illegal activity. Some may require the lien holder to file a timely claim in the confiscation process like any interested party, and the lien will be extinguished in the confiscation proceeding if such a claim is not filed. When the confiscation proceedings are complete and the asset is confiscated and sold, the creditor is paid from the proceeds.

Most of the APEC economies allow applications for provisional measures *ex parte* (without notice to the asset holder). Nevertheless, after a freezing order is issued the asset holder is usually given notice. China is an exception to this: once an account has been frozen, Chinese financial institutions are forbidden from disclosing the order.[146]

Especially in highly complex investigations, it may not be possible to wait until confiscation proceedings are carried out to deal with innocent third parties (e.g. mortgage holders, judgment creditors) who may have an interest relating to the property of the offender. One way to ensure they are compensated could be an interim sale ordered by the court. If it is decided to defer the issue to the final confiscation

proceedings, expenses may have to be paid with respect to the third parties' interests.[147]

B. "Provisional" Freezing/Seizure of Assets

In order to protect assets that may later be subject to confiscation, it is important that measures are taken as close to the beginning of a case as possible and secure the assets until the conclusion of the confiscation proceedings.[148] Although in some cases funds and property can be preserved through a restraint order enforced through an MLA request, other circumstances require greater urgency. For instance, if the target has been tipped off to the investigation through an arrest or leak, practitioners must act quickly to avoid the move of proceeds from one jurisdiction to another.[149]

To overcome this challenge, some economies have measures that enable a swift seizure or restraint of funds in emergency situations. This rapid action often takes the form of a temporary measure executed on the expectation that an MLA request will follow within a specified period of time. If the request is not provided in time, the asset may be released. An example of this is the United States legislation which allows for a temporary restraint order to be issued upon notice of charges being filed or an arrest in a foreign jurisdiction. The duration of the order is of 30 days and it is renewable.[150]

As restraining orders limit the use of property, jurisdictions typically require these measures to be judicially authorized. In many jurisdictions, however, emergency or short-term provisional measures can be implemented administratively, either through the financial intelligence unit (FIU), a law enforcement agency or other authority.[151] In Thailand, for instance, the Transaction Committee (an administrative authority) can order a provisional seizure or attachment of an asset, for a maximum duration of 90 days "if there is a reasonable ground to believe that any asset connected with the commission of an offense may be transferred, distributed, moved, concealed or hidden".[152] This is a recommended approach, as more time is needed to pursue an order from a court, during which the property might be concealed or lost. The rights of the owner must also be borne in mind. To this end, a possibility to appeal against the temporary freezing order and prove its legitimate source for it to be cancelled can provide sufficient protection.[153]

Some economies, such as Hong Kong, China, require an MLA request to obtain any provisional measure, but allow for hearings to be obtained on short notice and *ex parte*. Others may have stricter conditions, such as the requirement of an arrest or charges. In that case, practitioners may need to consider alternative options (initiating a joint

investigation, supplying enough information through informal assistance channels to enable provisional measures under domestic law). These options become possible when some element of the underlying crime is under the jurisdiction of the foreign authority[154].

Table 36: Types of Emergency Provisional Measures

SOURCE: Extract from StAR, *Asset Recovery Handbook. A Guide for Practitioners,* pp. 135-136.

Administrative orders. An administrative official (typically associated with the FIU) may issue a preservation order instructing a financial institution to restrain funds for a brief period of time. These administrative orders are sometimes limited to cases involving specified underlying offenses. Some jurisdictions operate under a "consent regime" that requires the financial institution, on the filing of an STR, to hold the funds until the FIU provides consent to release them or hold them for a specified period of time (thereby allowing the FIU or law enforcement to implement provisional measures).

Provisional orders of investigating magistrates. In civil law jurisdictions that have investigating magistrates, the magistrate may be able to issue orders authorizing provisional measures if there is reason to believe that a confiscation order may ultimately be issued, that assets are likely to be dissipated, or both.

Provisional measures on instigation of charges or arrest. Some jurisdictions permit a temporary restraint or seizure of assets subject to confiscation following an arrest in another jurisdiction. The requesting jurisdiction must provide evidence of the arrest and a summary of the facts of the case. The funds will be restrained to await further evidence, and this period of restraint can be extended on application. Generally, assets need not be traced to a crime and no treaty arrangement is necessary, and the proceeding is conducted without notice to the asset holder (*ex parte*).

Direct referral to prosecutors. In some jurisdictions, incoming requests for restraint and confiscation are referred to prosecutors to provide the same level of international cooperation in obtaining provisional measures and confiscating proceeds and instrumentalities of crime as is available in domestic cases. Evidence of crime and benefit or evidence that assets are proceeds or an instrumentality of crime may be required.

C. Freezing and Seizure of Assets

One of the requirements imposed by the UNCAC on its members is the need to include both of the systems for confiscation of assets contemplated in it: value-based and property-based[155]. Under the first system, orders are directed towards the person accused of committing an offense and related to the benefit obtained by them in

consequence. The property-based system uses asset-directed orders, which affect specific assets found to be the proceeds of crime or otherwise linked to the commission of an offense. These systems will be explained in more detail in Chapter IX.

In both systems, procedural rules on freezing and seizure of property may be outlined in confiscation laws or incorporate civil or penal procedure norms by reference. In common law jurisdictions the application for an order is usually done in writing, and comprises the seizure warrant or restraining order and the supporting affidavit. Civil law jurisdictions may require a recitation of the facts demonstrated by relevant documents or evidence contained in the case file before the judicial authority; likewise, the prosecutor or investigating magistrate may restrain or seize property based on the need to preserve evidence or avoid dissipation of assets subject to confiscation.[156] The assets subject to provisional measures will be those needed to satisfy the eventual confiscation order. Therefore, applications for provisional measures should be carefully crafted to correspond to the confiscation sanction pursued in each case.[157]

Person-directed and asset-directed orders have some basic requisites in common. Usually it is necessary that criminal proceedings (or confiscation proceedings, where they are independently available) have already been instituted, or are about to be, to issue an order. When applying for ne potential obstacle to freezing is the requirement that criminal proceedings be instituted in the requesting state. Some jurisdictions will freeze proceeds if criminal proceedings have been commenced or are about to be commenced. Others require reasonable grounds to believe that proceedings will be instituted and that confiscation may be ordered in those proceedings. The most demanding legislation may require a final conviction or a person and a final confiscation order in the requesting state.[158]

Additionally, there must be a risk of dissipation of the assets and, in some jurisdictions, undertakings may be required to ensure that costs and damages resulting from the failure of a confiscation order are paid.[159]

When the order will be issued by a Court, the application must be supported by evidence.[160] The standard of proof is that of an interim order,[161] and follows a “reasonable grounds to believe” or “probable cause” criteria.[162] It must be stressed that freezing and seizure orders are temporary measures, which can be lifted if legal requisites are not meet, made with the intention to preserve assets for future confiscation and avoid their dissipation and ; hence, the standard of proof need to be much less stringent than the applicable standard for a conviction at trial.

Table 37: Strategic considerations before drafting an order

SOURCE: "Freezing and Seizure Regimes", presentation by Mr. Guillermo Jorge, Partner at Governance Latam, APEC consultant, at the APEC Anti-Corruption and Transparency Working Group (ACTWG), *APEC Capacity Building Workshop: Designing Best Models on Prosecuting Corruption and Money Laundering Cases Using Financial Flow Tracking Techniques and Investigative Intelligence for Effective Conviction and Asset Recovery to Promote Regional Economic Integration*, Pattaya, Thailand, 22-24 September 2014.

- Asset management: Foresee the cost of management for each preliminary measure.
- Timing: Considering that the execution of an order will tip off the target and therefore dissipated assets not already identified, the appropriate timing to apply for an order is of strategic consideration.
- Third party involvement: Third parties –whether bona-fide or not- will usually confront freezing orders. Therefore, it is necessary to understand the background of the transaction to know whether a third party is applying in good faith.

1. Person directed orders

Person-directed freezing and seizure orders are employed in relation to value-based confiscation systems, which focus on the value of benefits derived from criminal conduct.

In such a system, when there is some evidence that the target has derived a benefit from an alleged offense, any asset under their control can be subject to a freezing or seizure order.[163] Most systems include assets that are effectively controlled, held, or gifted by the target. Some jurisdictions, however, limit confiscation to assets owned by the target. A strict interpretation of ownership can be problematic, given that in most cases assets are either owned by a company controlled by the target, or held in their benefit by a third party, or gifted by the target to a family member, associate or corporate vehicle.[164] Presumptions and broad definitions of ownership can be used to include assets controlled, held or gifted by a target.[165]

Some jurisdictions permit only the restraint or seizure of assets that are held by a target; and they define "held" broadly to include ownership and assets owned by others, but in which the target holds a beneficial interest. With regard to assets that are gifted, some jurisdictions permit the restraint or seizure of assets that have been gifted within a reasonable time, such as a five- or six-year period. These provisions are similar to the "claw back" provisions used to recover assets disposed of by a bankrupt person or entity in the period leading up to the bankruptcy.

The transactional activity surrounding assets should be evaluated to link a target to property held in the name of a close relative, an associate or a company. Factors to consider include:

- "the amount paid for the asset (market value), including whether a mortgage responsibility was transferred with the title;
- the source of funds used to purchase the asset;
- the person paying the expenses and outgoings associated with the asset;
- the capacity or resources of the owner of the asset to purchase or maintain the asset; and
- the person occupying, possessing, or controlling the asset".[166]

By considering these circumstances, evidence can be gathered that will permit a court to draw the inference that property held by a third party is in fact beneficially owned or controlled by a target. When the law permits, such assets could be subject to freezing or seizure measures, and eventually confiscation.[167]

Table 38: The Frigates Case (Chile)

SOURCE: "Freezing and Seizing Proceeds of Corruption", presentation by Ms. Claudia Ortega Forner and Mr. Antonio Segovia Arancibia, Legal Advisors at the Public Prosecutor's Office, Chile, at the APEC Anti-Corruption and Transparency Working Group (ACTWG), *APEC Capacity Building Workshop: Designing Best Models on Prosecuting Corruption and Money Laundering Cases Using Financial Flow Tracking Techniques and Investigative Intelligence for Effective Conviction and Asset Recovery to Promote Regional Economic Integration*, Pattaya, Thailand, 22-24 September 2014.

In the Frigates case, two former officials of the Chilean Navy and an arms vendor were charged for the alleged crimes of bribery and money laundering in the sale of four frigates to the Chilean Government in 2004. The relevant government contract would have been awarded to the arms vendor as a result of key information provided to him by the former navy officials –while they were employees of a state-owned shipyard – in exchange for improper payments. Both former officials jointly received deposits for a total of approximately $400,000 in their bank accounts from company related to the arms vendor.

The Prosecutor's Office and the State Defense Committee obtained a judicial order freezing the two former officials' bank accounts and all transactions involving their assets, for a total value of USD 892,385. Both former navy officials were sentenced to 5 years in prison and a USD 180,000 fine; their bank account balances were confiscated. The arms vendor died of illness before the investigation was finished; his company's property remains frozen.

2. Asset directed orders

Asset-directed orders for freezing and seizure are related to property-based systems of confiscation. These orders are aimed at assets connected to or found to be the proceeds or instrumentalities of crime. They require the establishment of a link between the property and an offense. When assets cannot be linked to an offense (e.g. the benefits are distanced from it through money laundering) this type of confiscation becomes more difficult. Some jurisdictions adopt regulations like substitute asset provisions or extended confiscation to overcome these obstacles (See Chapter IX).[168]

Assets used or intended for use in any manner or part to commit or facilitate the commission of an offense are known as instrumentalities of crime.[169]

Proceeds are defined by the UNCAC as any property derived from or obtained, directly or indirectly, through the commission of an offense.[170] Indirect proceeds are ancillary benefits that would not have accrued were if not for the commission of an offense. The definition of proceeds of crime in many economies includes direct and indirect proceeds. Some examples are Australia, China, Hong Kong, Indonesia, Japan, Malaysia, Papua New Guinea, the Philippines, Singapore and Thailand.[171]

Table 39: The Rudi Rubiandini Case (Indonesia)

SOURCE: "Best practices in freezing and seizing proceeds of corruption", presentation by Mr. Andi Suharlis, Prosecutor at the Corruption Eradication Commission, Indonesia, at the APEC Anti-Corruption and Transparency Working Group (ACTWG), *APEC Capacity Building Workshop: Designing Best Models on Prosecuting Corruption and Money Laundering Cases Using Financial Flow Tracking Techniques and Investigative Intelligence for Effective Conviction and Asset Recovery to Promote Regional Economic Integration*, Pattaya, Thailand, 22-24 September 2014.

Rudi Rubiandini was the Head of Indonesia Special Unit Upstream Oil and Gas Business. He received a bribe payment from a tender party to win an oil tender project. He used the proceeds of crime to buy a car, houses, a luxury watch, etc. His wife, sibling, and golf trainer were straw men.

When he was charged with money laundering, his house in South Jakarta, a BMW motorcycle and a Toyota Camry were seized. Local authorities also seized US$350,000 from his safety deposit box in a bank, as well as US$80,000 and 180 grams of gold from a strong box in his office. In 2013 he was sentenced to 7 years imprisonment and a US$ 17.391 fine or an additional jail term of three months. Money, a house, a car and a luxury watch were confiscated.

Given that asset-directed orders require proof that the property being sought is linked to criminal activities, there is no purpose in requesting a freezing or seizure order against an asset that cannot be characterized as the proceeds or an instrumentality of corruption, as previously defined, under this system.[172] In some jurisdictions, reverse onus provisions or rebuttable presumptions that some or all assets are proceeds of corruption may apply. Orders can be expanded to include the assets that would be confiscated by operation of the presumption.[173]

D. Obtaining Freezing Orders from another Member Economy

Asset recovery usually involves cross-border efforts. Funds and other property will frequently be located in a foreign jurisdiction, and it will be necessary to restrain them in order to avoid dissipation. In these cases, available administrative and emergency restraining orders should be considered as a first measure; ultimately, however, an MLA request will become necessary to retain freezing and seizure orders.[174]

An MLA request for restraint measures can be fulfilled either through the requested jurisdiction's "direct" enforcement of the requesting jurisdiction's order, or "indirect" enforcement. The indirect approach involves the application for a domestic order to restrain or seize assets in another member economy. When an application is made, the requesting jurisdiction must provide the evidence necessary to prove their case. The burden of proof and type of evidence required will be ruled by the requested jurisdiction's laws.[175]

The main disadvantage of the indirect method is delay. While assets such as funds in a bank account can be transferred very quickly, marshaling, transmitting evidence in support of the application and the hearing for the application itself can delay the process, enabling assets to dissipate quickly and making future confiscation difficult.[176]

In some economies, like Hong Kong, China and Singapore, restraint orders can be issued when confiscation proceedings have commenced (either in the requesting or the requested economy), and a confiscation order has been made or there are reasonable grounds to believe it will be.[177] Similarly, in Australia criminal proceedings or confiscation proceedings need to have started or about to be. An interim order is awarded under the Mutual Assistance in Criminal Matters Act 1987 until a foreign order can be registered. Alternatively, Australia can take domestic action under its Proceeds of Crime Act 2002 when an Australian court is satisfied there are reasonable grounds to suspect that the property is the proceeds of a foreign indictable offense and there is no requirement that overseas proceedings have been commenced or are imminent.[178]

Indonesia does not require evidence that proceedings have been or will be commenced in the requesting state;[179] Japan and Papua New Guinea do have such a requirement.[180] In Vietnam, a person must have been charged with an offense that may result in confiscation of the property[181].

E. Enforcement of Foreign Restraining Orders

Several APEC economies have attempted to overcome challenges in obtaining freezing orders by allowing direct enforcement of a foreign order. Under this approach, the requesting state obtains a freezing order from its courts and transmits the order to the requested state. The requested state then registers the foreign freezing order in its courts, after which the foreign order becomes enforceable in the requested state like a domestic court order. Time is saved because there is no application before the courts of the requested state for a second freezing order. This approach has proved to be timely, requires fewer resources, avoids duplication and is significantly more effective.[182]

Many economies do not allow for the direct registration of a foreign restraint order; among them are Indonesia, Japan, Malaysia and Singapore.[183] In Australia, a foreign restraining order on proceeds of crime reasonably suspected to be in Australian territory can be registered within their courts and directly enforced like a domestic court order. The order must relate to a serious offense. Papua New Guinea also allows for the direct registration and enforcement of foreign restraint orders.[184]

To further expedite the process, some economies permit registration of faxed copies of foreign orders. However, in most cases, a properly sealed or authenticated copy of the order must subsequently be filed.[185] Laws in Australia and in Papua New Guinea allow for the use of a faxed copy of a sealed or authenticated foreign order. Still, the registration ceases to have effect after 45 and 21 days respectively unless a sealed or authenticated copy is filed with the court.[186]

Direct enforcement of a foreign restraining order will not be possible in every case, as there may not be legal or treaty basis for direct enforcement in the requested jurisdiction. Some conditions usually necessary to give effect to these requests are:

- General requirements for MLA requests are met and there are no grounds for refusal.
- There are reasonable grounds to believe that the assets being sought are linked to the criminal activities, or that the target has committed an offense from which a benefit has been derived.
- There are reasonable grounds to believe the assets will be confiscated.
- The location of the assets to be restrained is provided.
- The relief sought could also be obtained if proceedings had been brought in the requested jurisdiction (or the assets subject to confiscation are also subject to confiscation in the requested jurisdiction).
- Copies (certified, if necessary) of relevant court orders are included, and are enforceable in the requested jurisdiction.[187]

Table 40: The Tan Sri Abdul Taib Mahmud Case (Malaysia)

SOURCE: Getting the Deal Through, *Asset Recovery 2015*, Law Business Research, p. 155.

In 2013, Malaysia launched a full-fledged investigation into Sarawak's Chief Minister, Tan Sri Abdul Taib Mahmud, for abuse of power and corruption. The allegations against him surfaced after a video released by Global Witness, 'Inside Malaysia's Shadow State', showed discussions between the Chief Minister's relatives and associates with an undercover investigator over the acquisition of Sarawak's forests.

Swiss authorities received information about property of Taib present in Switzerland, and initiated a move to freeze his assets while the investigation was still ongoing.

Table 41: The SNC-Lavalin Group Case (Canada)

SOURCE: Getting the Deal Through, *Asset Recovery 2015*, Law Business Research, p. 55.

In September 2011, the RCMP (Royal Canadian Mounted Police) initiated an investigation of corruption allegations against a company named SNC-Lavalin Group involving a World Bank funded bridge construction project in Bangladesh.

In April 2012 the Swiss authorities arrested a former executive vice-president of the company for participating in alleged payments to third parties relating to public contracts in Libya and Tunisia. They sent an MLA request to execute a search warrant in the company's headquarters. This led to obtaining evidence that the CEO of the company at that time had approved the payment of approximately C$56 million to unnamed 'agents' to help secure two contracts. He was arrested in November 2012 and charged with fraud and conspiracy. The former executive vice-president also faced domestic charges of corruption.

In May 2013, the RCMP asked a court in Montreal to freeze four bank accounts and a family trust belonging to another former executive vice-president of SNC-Lavalin Group, and also sought a freeze on a bank account of his in Cairo. The police claims he moved $23 million of his "proceeds of crime" from accounts in Switzerland to Canada, and used them to buy properties and fund a $13-million condo development in Montreal. Six properties in Montreal owned by the target and his children were frozen, and international authorities were asked to place a restraining order on a million-dollar condo in Florida.

The investigation on the SNC-Lavalin Group case is currently ongoing.

CHAPTER VIII. THE MANAGEMENT OF FROZEN ASSETS

Once assets have been secured through provisional measures, it will become necessary to preserve their safety and value until they are eventually confiscated or released. Freezing or seizure orders alone are not always enough to preserve property, which may deteriorate unless it is properly maintained and administered. In these cases, adequate asset management will be required to avoid devaluing of the assets.[188] For this reason, the United Nations Convention against Corruption (UNCAC) urges States to adopt the necessary legislative and other measures to regulate the administration of frozen, seized and confiscated property.[189]

When determining which assets should be subject to provisional measures, consideration should be given to asset management requirements generated by the proposed measure. A cost-benefit analysis should be made regarding assets that require management, as it is an expensive activity with the potential to cost more than the value of the asset being managed. As a general rule, if the estimated cost of maintaining, storing or managing property will exceed or substantially diminish the return on confiscation, assets should not be seized. In this respect, economies can establish value thresholds, for assets that are of low value or could depreciate.[190] Nevertheless, when reasons of public interest justify restraint measures (e.g. in the case of an abandoned house used for illegal activity) the general rule may not apply. There may also be reasons to allow the use of an asset (for example, when a family home is subject to a restraint order). Finally, certain assets can be preserved without the need to appoint an asset manager (for instance, registering a lien on land in the public records), which reduces expenses, complexity and administrative work.[191]

Furthermore, economies should bear in mind the need for transparency and security in the management of seized assets. Unfortunately, they sometimes lack regulations on the matter.[192] Clear policies in relation to these matters should be developed and communicated to practitioners and asset managers for the asset recovery process to be effective.[193]

A. Asset management authorities

Asset management can be carried out by a variety of agents. In some economies, like Hong Kong, China[194] and the Philippines,[195] an asset manager will be appointed specifically when necessary; other economies make use of existing administrative

structures to fulfill this role, or possess specific asset management entities, as it is the case of Australia,[196] Canada,[197] United States,[198] and New Zealand[199]; law enforcement agencies and courts can also participate in management.[200]

Asset managers need a specific skillset, including the ability to (i) preserve the security and value of assets pending confiscation (including the sale of rapidly depreciating assets); (ii) hire contractors with specialized skills to accomplish management tasks when necessary; (iii) liquidate assets for a fair price after confiscation; and (iv) distribute the proceeds in accordance with applicable legislation following payment of all necessary expenses. It should not be assumed that courts, prosecutors and law enforcement officials in preexisting structures already have the required skills and resources. Although there may be some basic capacity in this area—for example, a law enforcement agency seizes and stores property that is evidence of criminal offenses—these systems are insufficient to deal with the seizure or restraint and confiscation of a wide range of assets. Expertise on the matter can be obtained from other sources.[201]

Table 42: How to obtain the necessary management expertise

SOURCE: StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 92.

• Creating a separate specialized asset management office: Set up an agency with responsibility to manage seized or restrained assets, hire qualified asset managers, conduct pre-restraint planning and analysis, and coordinate post-confiscation realization or liquidation.
• Creating an asset management unit within an existing agency: In some cases, a new unit dedicated solely to the duties of managing assets subject to confiscation is established within an existing government agency. Logically, this is often an agency with ready expertise in asset management.
• Outsourcing asset management: In those jurisdictions where establishing an asset management office or co-opting an existing agency is not an option, engage private, locally available property trustees.

The asset manager must be involved in consultations with other practitioners that take part in the asset recovery process (law enforcement officers, financial analysts, prosecutors and investigating magistrates) as regards management decisions. This may be beneficial when a decision can affect the value of the restrained assets, by mitigating claims for losses due to mismanagement; especially if consultations involve targets, interested third parties and the applicant for the restraint order. Considerations

made by all parties should be taken into account and recorded in writing; however, the final decision shall be made by the asset manager, subject to the direction of the court.[202]

Table 43: Case Studies: Canada, New Zealand and the United States

SOURCE: Public Works and Government Services Canada, Seized Property Management Directory, 2012, available at http://www.tpsgc-pwgsc.gc.ca/app-acq/gbs-spm/index-eng.html; New Zealand Insolvency and Trustee Service, Criminal proceeds management, 2013, available at: http://www.insolvency.govt.nz/cms/site-tools/about-us/proceeds-of-crime; United States Department of Justice, Participants and Roles, 2013, available at: http://www.justice.gov/jmd/afp/05participants/index.htm; United States Marshals Service, Asset Forfeiture Fact Sheet, 2015, available at: http://www.usmarshals.gov/duties/factsheets/asset_forfeiture.pdf.

Canada

The 1993 Seized Property Management Act authorizes the Canadian Minister of Public Works and Government Services to: provide consultative and managerial services to law enforcement agencies in relation to property seized or restrained in connection with designated criminal offences; dispose of this property when the Courts declare forfeiture; and share the proceeds of the disposition. The Seized Property Management Directorate (SPMD) of Public Works and Government Services Canada (PWGSC) manages assets seized or restrained under specific sections of the Criminal Code, the Controlled Drugs and Substances Act and the Proceeds of Crime (Money-laundering) and Terrorist Financing Act.

Before assets are seized, the SPMD provides advice to police agencies and prosecutors on their value and the estimated costs of management, analyzes the best method to preserve them, and coordinates services such as towing, storing and inspection, as needed. Once an asset has been seized by the police and an order of management or restraint has been issued by the appropriate judicial authority, the SPMD takes possession and control of the reported seized assets or manages the restrained property, in accordance with the order. It is in charge of the inspection, appraisal, administration, storage, protection and maintenance of the seized or restrained property. The SPMD, in consultation with the Department of Justice, settles third-party claims on seized property. It also advances funds to preserve property.

New Zealand

The Criminal Proceeds Recovery Act of 2009 (CPRA) establishes New Zealand's forfeiture of property regime. The Official Assignee for New Zealand is the statutory authority under the CPRA for custody and control of property restrained or forfeited by the Court. Assets are managed by the OACU (Official Assignee Compliance Unit), which seizes, inspects, stores, preserves, maintains and administers restrained property. Regular appraisal and inspection of property, payment of certain costs derived from the preservation of property and the sale of assets on orders from the Court are also part of the OACU's functions.[203]

When the appropriate appeal period or a specified period of 6 months has passed, the OACU normally disposes of moveable assets through a public auction. Cash is banked into a trust account, and real property is usually sold through appointed local agents on the open market. The OACU will also arrange for the necessary transportation of moveable assets and valuations of assets to monitor equity preservation and costs associated with the management of certain assets.

United States

Seizure and forfeiture of assets that are proceeds or instrumentalities of crime in the United States is carried out by the Department of Justice (DoJ) through its Asset Forfeiture Program (AFP), created in 1984. Within the DoJ, the United States Marshals Service is in charge of the custody, management and disposal of the majority of the property seized for forfeiture.[204] As of September 2013, the Marshals Service was administering assets for a total value of USD 2 billion. During fiscal 2013, USD 200 million were distributed to claimants and victims of crime, and USD 571 million were shared with participating state and local law enforcement agencies. Proceeds obtained from asset sales are used to fund the AFP, compensate victims, and supplement funding for law enforcement initiatives and support community programs.[205]

In addition, the Asset Forfeiture Management Staff (AFMS) within the DoJ is responsible for the management of the Assets Forfeiture Fund, the Consolidated Asset Tracking System (CATS), program-wide contracts, the oversight of program internal controls and property management, the interpretation of the Assets Forfeiture Fund statute, the approval of unusual Fund uses, and legislative liaison on matters affecting the financial integrity of the AFP.[206]

B. Powers and duties of the asset manager

The asset management office or authority must be given legal powers to carry out various requisite functions when placed in control of assets. Typically, they are granted through existing laws on confiscation, asset management, anti-money laundering, and rules of the court. They include:

- "authority to pay all necessary costs, expenses, and disbursements connected with the restraint or seizure and the management of the assets;
- authority to buy and sell seized or restrained assets that are in the form of shares, securities, or other investments;
- authority to insure assets under control;
- in the case of a business, authority to operate the business, including to employ or terminate the employment of people in the business, hire a business manager if required, and make decisions necessary to manage the business prudently;
- in the case of assets that represent shares in a company, authority to exercise rights in respect of those shares as if the asset manager were the registered holder of those shares; and
- authority to pay salaries of the asset manager and people involved in asset management, in accordance with a defined scale or regulation, or in accordance with an order of the court that is subject to full disclosure and mandatory audit".[207]

If confronted with any management issue for which no specific powers are given in the legislation, the asset manager may need to request the guidance and authority of the court that issued the restraint order, which can be time-consuming and costly.[208]

Information-gathering powers are sometimes available to asset managers, particularly in relation to property of which the exact nature and location is unknown, or to enforce value-based orders. They may allow for production orders, search warrants, compulsory statements by targets, and examinations. A useful tactic that can be used in both common and civil law systems is ordering a target to disclose to the asset manager in a sworn statement the nature and location of his or her assets. Even the refusal to make a statement can be useful to the investigation (for example, to defend against an application from the target to have access to restrained property to pay for legal fees or living expenses).[209]

It is essential for the asset manager to keep detailed records of the restrained assets and any transactions involving them. A thorough inventory of the assets and the condition they are in should be made and updated frequently, including appraisals of the property. Photographic or video evidence of the asset's condition at the time the restraining measure was imposed should supplement the records. This information serves to protect the asset manager of subsequent claims of responsibility for property damage. Any management issue or defects identified at the time of restraining should as well be informed to the court, the prosecutor or both, so that appropriate measures are taken and the asset manager is not blamed for pre-existing conditions.[210]

Reporting is important as it increases the transparency of asset management and may raise public awareness of its purpose and benefits. Reports on specific cases to the court or the applicant for a restraining order may be mandated by regulations. The inventory and valuation should be attached to reports. Additionally, annual reports on the asset management unit's activity and statistics may be required.[211]

C. Management challenges of specific assets

- **Cash, bank accounts and financial instruments**

Money is relatively easy to manage once restrained. Bank accounts can be frozen; the possibility that a rigid preservation order will impact outstanding payment instructions, mortgage obligations, loan payments and similar obligations should be considered.[212] Cash (except when it is used as evidence) can be preserved in an interest-bearing account. Financial instruments (such as cashier's checks, money orders, certificates of deposit, stocks, bonds, and brokerage accounts) can be seized and will require measures to preserve or redeem their value. A professional (i.e. a stock broker) should conduct a valuation of stocks, bonds and brokerage accounts, and determine how best to preserve them.[213]

- **Real property (Land)**

Real property is generally a good type of asset to seize for confiscation purposes. In jurisdictions with an efficient land ownership system, which keep a registry of ownership and encumbrance details, a lien or other notice of encumbrance can be inscribed in the public records. This gives sufficient notice to any potential purchaser to whom the target may attempt to sell the property. Even with a restraint order in place, failure to register the encumbrance would not prevent a bona fide third party from buying it and later claiming bona fide ownership.[214]

Though land can often be restrained without the need to appoint a manager, several problems can occur:

- Land can be subject to government rates and taxes, and it may be encumbered to banks as security for mortgages or loans. A court order should require the target to maintain current payment of taxes and other debts that have the potential to encumber the land with a lien, and the court should be alerted if he or she stops paying. Alternatively, the right of the target to continue occupying the property could be made conditional on the payment of these expenses, and the manager could be authorized to evict them if the conditions are not met. If eviction became necessary, the asset manager may seek to lease the asset at a rate that covers expenses, or sell the property and use the proceeds to cancel any debts.
- Land may generate heavy, property-related expenses and utility bills, some of which may be urgent. Some types of land require expensive maintenance to retain their value—for example, a golf course or farm. Funds could be obtained from the target's assets, a designated confiscation fund, or some other contingency fund. If this was not possible or insufficient to maintain the property, it could be sold or leased where permitted.[215]

❖ **Motor vehicles, boats and airplanes**

Vehicles are difficult and costly to store and maintain, and the period between seizure and confiscation can last for years. In addition, vehicles depreciate quickly. Preserving this type of asset requires a secure and appropriate storage facility where proper maintenance may be provided by people with the adequate expertise. They must not simply be left in a yard outside, as this could expose the management agency to compensation claims and substantially reduce the assets' value. Expert maintenance and proper storage will be expensive; hence, financing should be planned beforehand.[216]

Given the nature of these assets, when they are old or in poor condition seizure may not be justified. If they are relatively new and in good condition, they could be sold if permitted. The target could also be allowed to use the vehicle during the confiscation proceedings if he gives a guarantee for the payment of a value equivalent to the one it had at the time the case was initiated.[217]

❖ Businesses

Effective restraint of businesses typically calls for the appointment of an asset manager. To decide if restraint is advisable, an equity valuation of the business should be undertaken before any measure is requested (or shortly after) to accurately determine its debt load and equity. Businesses with little value may be best closed or sold, without undertaking the financial risks derived from its operation. Moreover, identifying the business as a target for confiscation can possibly damage its goodwill value. To prevent this, the current manager could be allowed to continue its operation, but under the control of a business manager contracted by the asset manager or appointed by the court.[218]

Pre-restraint planning is crucial in relation to businesses. To avoid the removal of business assets and cash, restraint orders should be made *ex parte*. Once restrained, appointed experts should immediately assume control of the business. They should immediately take control of bank accounts, accounting systems and records, important business data (such as customer records), valuable stock, and valuable plant and equipment. When operation of the business will continue, books and accounting records must be made available and should be assessed by the manager. In addition, managers will need to engage with staff and key personnel, and evaluate the reliability of those employees. Removal of staff may prove costly and can result in loss of corporate knowledge, customer dissatisfaction, and loss of business; however, retaining staff who respond to the target can affect the business as well. Regular reports on the performance of the business should be sent to the prosecution agency responsible for the restraint order, and any problems with the business should be raised immediately.[219] The involvement of innocent partners in the business should also be considered, in order not to affect their interests.[220]

❖ Livestock and farms

Managing animals is often quite problematic. When these assets are of very high value to certain markets (for example, race horses can be worth hundreds of thousands or even millions of dollars), practitioners are more inclined to include them in restraint orders. However, the costs for stock-feed, veterinary procedures, yard and pasture maintenance, and staffing are also high. As sufficient revenue streams to fund these expenses are unlikely, some jurisdictions refuse to seize livestock and farms. Others may be authorized to restrain the farm, then seize and sell the livestock (with or without consent of the owner). Alternatively, a bond could be posted if a target or associates desire to continue the operation during confiscation proceedings.[221]

❖ **Precious metals, jewels and artwork**

These assets should be carefully inventoried and stored in a secure facility. They require inspection, verification and valuation to be done by an expert.[222]

❖ **Perishable and depreciating assets**

This category of assets generally includes:

- highly perishable assets, which lose all value if not sold within a few days (e.g., a boatload of fresh fish or a consignment of cut flowers);
- moderately perishable assets (such as a field crop or farm animals) that will lose value if they are not sold at an appropriate time, possibly within weeks or months;
- depreciating assets, including cars, boats, and electronic equipment that lose 15 to 30 percent of their value each year.[223]

When dealing with depreciating or perishable assets, asset managers can be given authority to effect an interlocutory sale prior to a final confiscation order and place the proceeds in an interest-bearing account supervised by either the asset manager or the court. One example of this is Japan, where assets that are inconvenient to be kept can be sold, and the proceeds are kept in substitution.[224] Interlocutory sales can also be conducted in the Philippines, for perishable or depreciating assets, or property that is excessively expensive to keep.[225] Where such powers are not available, an order to that effect can be requested to the court. Consent of all parties is preferable, but the court should have authority to enter such orders even if contested.

❖ **Assets Located in Foreign Jurisdictions**

Assets may be restrained and seized by foreign jurisdictions through informal assistance (like administrative avenues) or an MLA request. Enforcement of the restraining order will be under the responsibility of the authorities in the foreign jurisdiction; which can designate an asset manager to this end.[226]

Generally, the asset managers in both jurisdictions will work together to maintain the assets. It is wise anyway to ensure that the asset manager in the requesting jurisdiction has additional powers to help enforce the foreign restraint order and manage the assets. He or she will have no physical control over the assets in the requested jurisdiction, but will be permitted to hire contractors, lawyers, and other agents in the requested jurisdiction to obtain orders from its courts.[227]

Some possible issues include the possibility that the requested jurisdiction lacks authority to restrain a certain type of asset (such as livestock), or does not have an asset manager or specific funds. Discussions with the requested jurisdiction can help resolve them.[228]

Table 44: Management of a seized "animal fighting venture" (United States)

SOURCE: StAR Initiative, *Stolen Asset Recovery: A Good Practices Guide for Non-Conviction Based Asset Forfeiture*, 2009, Box 30, p. 89, available at: https://star.worldbank.org/star/sites/star/files/Non%20Conviction%20Based%20Asset%20Forfeiture.pdf

In the United States, Title 7 United States Code, Section 2156 (f) declares animal fighting ventures illegal and provides for the forfeiture of animals involved in them. Animals involved in these ventures are trained to fight each other until one of them is killed, and bets are placed on them in fights.

While executing a search warrant at one of the homes of a professional athlete, law enforcement seized various items and equipment associated with an illegal dog fighting venue, including approximately 53 pit bulls. Most forfeiture statutes in the United States allow the government to determine the disposition of forfeited property. In this case, however, it must be determined by the court. Prosecutors decided to appoint a special master to evaluate the dogs' temperament and medical condition, and determine the available options.

The cost of housing and caring for the dogs, the fees for the medical assessment and the special master added up to USD 100,000. Interim costs were covered by the Asset Forfeiture Fund, and later reimbursed by the claimant as part of his guilty plea agreement in the related criminal case. 50 of the dogs were saved from euthanizing because of the specific provisions allowing for forfeiture, the adequate funding and the subsequent shift of costs to the claimant. Some of the dogs were placed in an animal sanctuary, and the ones that met the necessary behavioral criteria could be placed in homes.

D. Funding asset management

Asset management is an expensive process, which requires predictable, continued and adequate financing. In ideal circumstances, expenses made to preserve the value of the assets can be paid from income generated by them (e.g. seized cash, profit from a business, sale of depreciating assets). When no cash or income is available, funds can be obtained by selling the property, from the target, from the proceeds of confiscation or a confiscation fund.[229]

Asset forfeiture funds have been established by many economies to overcome a chronic underfinancing of asset management, derived from difficulties in estimating budgetary requirements beforehand and deliberate choices by some decision makers to impede investigations. These funds are usually established through specific legislation that allocates the proceeds generated by asset forfeiture to designated law enforcement purposes for case-related and programmatic expenses, including the purchase of equipment, training, investigative expenses, prosecutorial and property management and liquidation costs. Using the proceeds of crime to fund law enforcement ensures that a program can be self-sustaining, while also conveying a symbolic message to criminals.[230]

Currently among the APEC economies Australia,[231] Canada, Chile, Thailand and the United States have specific forfeiture funds. The Philippines and Mexico do not; in Mexico, the Government distributes the forfeited funds to the ministries responsible for health, law enforcement, and the judiciary, in equal shares.[232]

Forfeiture funds have been recommended in the interpretive notes to the FATF Forty Recommendations on Money Laundering, the Commonwealth Model Legislation, The OAS Model Regulations and the G8 Best Practices for the Administration of Seized Assets.[233]

Legislation creating a forfeiture fund should specify the source of deposits, which agency will have the authority to administer this fund, and which expenditures can be paid from the fund. Economies may want to allocate part of the deposits to the national treasury, give authority to share property with foreign governments, allow interlocutory sale of assets and the use of funds to pay victims of crime.[234]

Table 45: Risks and possible solutions in asset forfeiture funds

SOURCE: StAR, *Stolen Asset Recovery: A Good Practices Guide for Non-Conviction Based Asset Forfeiture*, Box 32, p. 94

Potential Risks	**Solutions**
Improper targeting of individuals for purposes of seizing assets for personal gain or institutional purposes.	Senior-level supervision over case initiation and seizure approvals. No direct payment of salaries of investigators and prosecutors involved in the seizure process. Salaries of property

	managers, analysts, and support staff are appropriately paid from fund receipts. No personal incentives or rewards from seized assets.
Fund misuse in jurisdictions with weak financial management, especially in jurisdictions with endemic corruption.	External auditing, transparent reporting, practice guidelines, periodic statistical reports, all of which would be publicly available.
Reduction of appropriated funds in anticipation of forfeiture revenue.	The enabling legislation for a forfeiture fund should state that forfeited assets are used to supplement appropriated funds, not replace them.
Operation of a forfeiture fund imposes additional costs on government.	An adequately funded forfeiture program will offset the costs to government. Additional benefits of a segregated fund include better oversight and greater opportunity to protect against misuse.

E. Expenses, use and sale of restrained assets

In certain cases funds from the restrained assets will be destined for the living, legal, and business expenses of a target and his or her dependents. Though in most cases these expenses will be determined by law or fixed by the court, occasionally the asset manager will be involved in establishing what constitutes “reasonable” expenses. These decisions and any transaction in connection with them should be recorded, as they are usually disputed before the courts.[235] In some cases, targets will abuse this provision to strip restrained assets of their value. Economies can respond to this by limiting the maximum amount for expenses that can be claimed, or leaving it to the discretion of the court. Sometimes the only way to fund these expenses will be the interlocutory sale of the property; the applicant for the expenses order should expect that the court may mandate the sale of assets to fund the order.[236]

A target may have massive debts. Creditors can attempt to collect judgment liens or force the target into bankruptcy, thereby competing with the confiscation objective. Under these circumstances, the asset manager should consider how the provisions in the confiscation regulations relate to the ones in the bankruptcy legislation in the corresponding economy.[237]

Ethical and financial reasons advise against the use of property that has been seized but not yet confiscated. If authorities are immediately allowed to use any assets in the preliminary stages of the process, they may have little incentive to pursue a confiscation until its conclusion. This would effectively deprive targets of their property without a court judgment. Furthermore, provisional-use practices create an unwanted incentive for law enforcement to seize assets without necessarily showing the required evidence. Finally, the asset's value may diminish because of the use.[238] Some economies, such as China, Japan and the United States, deny the use of seized assets to authorities.[239]

Normally, the asset manager's role is limited to the preservation, maintenance and management of property, and only involves sale before a confiscation order in relation to perishable assets. When assets need to be sold, the most transparent procedures available should be preferred, so as to minimize allegations of mismanagement. Generally, this consists of a well-advertised and professionally-run public auction. In case property is of a specialized or exotic type, different methods (such as sales to specialized markets) can be employed to obtain the maximum price. Decisions in this aspect should be the subject of expert advice and well documented.[240]

Fees paid to the asset manager are usually established in asset confiscation norms as deductible from the confiscation proceeds, either on a fixed percentage or fee-for-service basis. It is good practice for the manager to provide regular updates of his or her fees to the prosecutor, so it can be assessed whether the order is becoming uneconomical. In some cases, fees cannot be deducted (for instance, when confiscation proceedings are discontinued or unsuccessful). The manager fees will then have to be paid by the confiscating authority, which can use any existing confiscation fund. Good practice suggests that an agreement be made on these matters as early as possible in the asset recovery process, to avoid later disputes.[241]

Table 46: Case Study. Thailand's Asset Management System

SOURCE: StAR Initiative, *Stolen Asset Recovery: A Good Practices Guide for Non-Conviction Based Asset Forfeiture*, 2009, Box 30, pp. 167-171.

The Anti-Money Laundering Office (AMLO) was created in Thailand in 1999 as an independent law enforcement and regulatory agency, under the supervision of the Ministry of Justice, which serves as the member economy's financial intelligence unit. AMLO's Asset Management Bureau is in charge of the custody, management and disposal of seized or forfeited assets.

The Asset Management Bureau's responsibilities include registering and appraising seized or attached property, storing, maintenance, return of released assets, appointing managers, handling the use of property by claimants, and overseeing auctions of assets, among others.

Management considerations are made before executing a search and seizure operation. The officer who seized the property will deliver it to the Asset Management Bureau for inspection and classification. Cards are attached to each item indicating relevant details of the property (name, category, quantity, size, weight, condition, and date of seizure). Later, the property is secured in appropriate places. When property would be difficult to manage by AMLO, an expert can be hired to do it. When assets are unsuitable or burdensome to keep in custody, AMLO's Secretary general can either: authorize the owner of the asset to hold it provisionally with bail or security; sell the property by auction before conclusion of the forfeiture proceedings; or allow law enforcement or other government agencies to provisionally use the property for official purposes.

AMLO uses information technology software called the Consolidated Asset Tracking System (AMCATS) to record and track all data relevant to restrained assets in a transparent manner. The AMCATS records the asset's name, value, name of the related case, seizure order, storage location, income generated and maintenance expenses. When appropriate, details of the auction or official use of the asset are included. The software allows AMLO to easily produce reports and statistics, maintain an inventory and control expenses.

In 2008, an asset forfeiture fund was created to facilitate efficient and cost-effective asset management and provide resources for forfeiture programs. After property is forfeited, part of the proceeds goes to the benefit of the national treasury, and the remainder is deposited in the Anti-Money Laundering Fund. It may be used for a range of purposes, such as providing resources for asset tracing and management, increasing public awareness, conducting training, and supporting international cooperation.

Table 47: The Ferdinand Marcos Case (Philippines)

SOURCE: JIMU, I., Basel Institute on Governance, International Center on Asset Recovery, *Managing Proceeds of Asset Recovery: The Case of Nigeria, Peru, the Philippines and Kazakhstan*, 2009, pp. 12-13.

Ferdinand Marcos was President of the Philippines from 1965 to 1986. He was removed from power by the 'people power revolution' on allegations of corruption. It is estimated that he misappropriated between USD 5 and 10 billion from government contracts. He employed various means, such as the takeover of large private enterprises, the creation of state-owned monopolies in important sectors of the economy, the awarding of government loans to private individuals acting as fronts, the raiding of the public treasury and government financial institutions, the receipt of kickbacks and commissions from firms working in the Philippines, and the diversion of

foreign aid and other forms of international assistance. The proceeds were laundered through shell corporations, which invested the money in real estate in the United States, or by depositing the funds in various domestic and offshore banks under pseudonyms, and in unnumbered accounts or accounts with code names.

In Switzerland, for instance, the amount hidden and frozen at the time Marcos left office was USD 356 million. In 2004, this amount plus the accumulated interest were returned to the Philippines' Treasury. The Swiss authorities, through the Zurich cantonal attorney, oversaw the choice of investments that could be made from the account while the funds were in the escrow account in the Philippines National Bank. The monies were later transferred to an off-budget fund known as the 'Agrarian Reform Fund', meant for land acquisition and distribution (LAD) and support services.

A number of transactions involving the fund have been questioned. In October 2006, the Commission on Audit reported that a significant portion of the Marcos funds had been used to finance excessive and unnecessary expenses that were unlikely to benefit the intended beneficiaries of the agrarian reform. Some of the money was also spent on items unrelated to priority projects, while other amounts were spent on procuring items at inflated prices. Furthermore, the Swiss Court's decision related to the Marcos case required that one third of the returned monies should be distributed to the thousands of Filipinos who were victims of human rights violations under Marcos' dictatorial regime. To this day, they have received no compensation and taken no action as to the allocation of the money. A bill was drafted to this end in 2003, and passed by the Senate in 2007, and is still pending of passage in the Chamber of Deputies.

Table 48: The Vladimiro Montesinos Torres Case (Peru)

SOURCE: JIMU, I., Basel Institute on Governance, International Center on Asset Recovery, *Managing Proceeds of Asset Recovery: The Case of Nigeria, Peru, the Philippines and Kazakhstan*, 2009, pp. 11-12.

Vladimiro Montesinos Torres was head of Peru's secret service (*Servicio de Inteligencia Nacional* - SIN) and advisor to the *de facto* president Alberto Fujimori between 1990 and 2000. During this period, corruption in the State structures was endemic. Montesinos was found to be at the center of a multi-million dollar illegal business, responsible for the extortion of high profile entrepreneurs, embezzlement, graft, arms trading, and drug trafficking. He used shell companies to launder the proceeds to other jurisdictions. Close to USD 2 billion are estimated to have been stolen during Fujimori's rule. Since Montesinos' conviction, USD 185 million have been recovered, in total, from the Cayman Islands, Switzerland and the United States; though it is known that Montesinos operated bank accounts in other jurisdictions.

The government of Peru created the *Fondo Especial de Administración del Dinero Obtenido Ilícitamente en perjuicio del Estado* - FEDADOI (Special Fund for Management of Illegally Obtained Money to the detriment of the State) to manage the assets recovered from corrupt officials by the government. A board of five members,

from different government ministries, manages the fund, and guidelines and detailed proceedings are defined to ensure the transparent use of the recovered assets. So far, however, money has mainly ended up supplementing the budget of the Institutions that have a member on the board. Moreover, since the spending items are not clearly set out in advance, questionable spending allocations occur often. Funds have been destined to the payment of vacations, purchase of new uniforms and life insurance for police personnel; legal fees towards the repatriation of Alberto Fujimori from Chile, reparations to the victims of misrule during the Fujimori rule, and investments in information technology and infrastructure for the judiciary.

CHAPTER IX. CONFISCATION PROCEEDINGS

Restrained assets are usually seized or frozen with the purpose of being confiscated. The term “confiscation” refers to the permanent deprivation of assets by order of a court or other competent authority.[242] This action impedes the enjoyment of illegal gains and, when possible, guarantees compensation for the victims of the crime.[243]

A. Methods of Confiscation

Confiscation may be property or value based. Both approaches target proceeds of crime, and there is a large overlap between the operational reach of the laws. However, they differ in the procedures used and the evidentiary requirements for obtaining these proceeds.[244]

Property-based systems (also referred to as “in rem” confiscation or “tainted property” systems) allow the confiscation of assets found to be the proceeds or instrumentalities of crime (assets used or intended for use in any manner or part to commit or facilitate the commission of an offense).[245] Therefore, the investigator will have to link the assets with the offense. Proceeds of crime are defined by the UNCAC as any property derived from or obtained, directly or indirectly, through the commission of an offense[246]. Indirect proceeds are ancillary benefits that would not have accrued were it not for the commission of an offense. In economies such as Australia, China, Hong Kong, Indonesia, Japan, Malaysia, Papua New Guinea, Philippines, Singapore and Thailand the definition of proceeds of includes both direct and indirect profits.[247]

A weakness of the property-based system is that the connection between the assets and the offence could be difficult to prove when assets have been laundered, converted, or transferred to disguise their illegal origin, or when the target has not directly participated in the criminal activity.[248] Some jurisdictions adopt regulations like substitute asset provisions or extended confiscation to overcome this obstacle[249]. Substitute asset provisions enable the confiscation of assets not connected to the offense, when the target is found to have dissipated the original assets and they cannot be found[250]. Extended confiscation is used to allow confiscation of assets that are benefits of similar or related criminal activities, with sufficient connection to the offense[251]. It is appropriate then, to distinguish between direct proceeds and indirect proceeds.

Value-based systems (also referred to as “benefits” systems) allow the determination of the value of the benefits derived from crime and the confiscation of an equivalent value

of assets that may be untainted. Some jurisdictions use enhanced confiscation techniques, such as substitute asset provisions or legislative presumptions to assist in meeting the standard of proof.[252] The total amount of the benefit obtained can be subject to confiscation, whether or not the assets confiscated have any link to the offense. In this system, there is a quantification of benefits which flowed to the defendant from the offense (direct benefits) and most often any increase in value due to appreciation of the assets (indirect benefits),[253] which is used later to impose a liability equal to the defendant's benefit. Furthermore, in some economies, the existence of benefits may be inferred from increases in the value of assets held by the target before and after the commission of an offense.[254]

Table 49: The benefits in value-based systems

SOURCE: StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 112.

The benefits will usually include:

- the value of money or assets (including "illegal" assets) actually received as the result of committing an offense;
- the value of assets derived or realized (by either the defendant or a third party at the direction of the defendant) directly or indirectly from the offense;
- the value of benefits, services, or advantages accrued (to the defendant or a third party at the direction of the defendant) directly or indirectly as a result of the offense (for example, the value of the lavish entertainment in a bribery case; or of forced manual, household, or other labor in a human trafficking or smuggling case); and the value of benefits derived directly or indirectly from related or prior criminal activity.

The advantage of this system is that the investigator does not have to link the specific assets to an offence. Nevertheless, he will have to connect the benefits with the offence that form the basis of the defendant's conviction which can be problematic when the prosecutor proceeds on only some of the offenses. To circumvent this drawback two approaches have been developed: one is the implementation of representative charges that capture a continuing course of criminal conduct over a period of time (which will permit an order for confiscation for all the benefits derived from that course of conduct over the entire period). The other one is the implementation of rebuttable presumptions (which can allow the inference that benefits derived over and extended specific period of time are benefits of that offense) and extended confiscation (that will permit the court to include any related or similar criminal activity in calculating benefits).[255]

The main weakness of the system is that the assets that can be confiscated are those owned by the defendant. To overcome this obstacle legal presumptions and broad definitions of "ownership", which include assets that are held or controlled by the defendant, are used.[256]

Some APEC economies, such as Australia; Brunei Darussalam; Canada; Hong Kong, China; Japan; Malaysia, Singapore and the United States, employ both systems, permitting confiscation of identified assets and a judgment that can be satisfied from the legitimate assets of a person.[257] Indeed, international standards recommend the implementation of both types of confiscation.[258]

In order to increase the effectiveness of the confiscation system or capture an extended range of assets, certain procedural aids or enhancements can be used:

- rebuttable presumptions: consist of an inference of the truth reached through a probable reasoning, which main consequence is to shift the burden of proof. The presumption is converted into an uncontroverted fact if the party against whom the presumption exists fails to overcome it. They are not frequently used in criminal proceedings but are more common in civil proceedings. There are different types of presumptions:
    - possession: assets in the possession of a person at the time of the offense, or shortly before or after the commission of the offense, are considered to be either the proceeds or an instrumentality of the offense;
    - associations: assets belonging to a person who has participated in or supported a criminal organization are presumed to be at the disposal of the organization and can be confiscated;
    - lifestyle: when the prosecutor can show that the off ender does not have sufficient legitimate sources of income to justify the value of assets accumulated over a period of time;
    - transfers of assets: presumption that transfers to family and close associates or any transfers for below-market value are not legitimate. In Thailand, for example, transfers of property to family members are presumed to be dishonest.[259]
    - nature of the offense: linked to conviction for a class of particularly serious offenses.[260]

  Some economies, for example Australia, have reserved the application of presumptions to serious offenses[261]. Canadian Criminal Code, Section 462.39,

provides that for the purposes of forfeiture orders, “the Court may infer that property was obtained or derived as a result of the commission of a designated offence where evidence establishes that the value, after the commission of that offence, of all the property of the person alleged to have committed the offence exceeds the value of all the property of that person before the commission of that offence and the court is satisfied that the income of that person from sources unrelated to designated offences committed by that person cannot reasonable account for such an increase in value.[262]

- Substitute asset provisions: permits the confiscations of assets not connected to the offense. It is mainly useful in property-based systems. It may be necessary to prove that the original assets were derived as a benefit of an offense, or that an asset was used as an instrumentality and that the asset cannot be located or is unavailable. In the United States, substitute assets may be confiscated in most criminal confiscation cases, but not through non conviction based confiscation.
- Extended confiscation: permits courts to confiscate assets derived from similar or related criminal activities, even if the offender is not charged for those other related activities.
- Other mechanisms to void transfers of assets: some economies, such as the United States, have enacted statutory provisions that hold that, at the time of the unlawful act, the state or government had title to the confiscated assets, which permits its confiscation.
- Automatic confiscation on conviction: confiscation by automatic operation of the statute. However, the person who claims an interest in an asset subject to automatic confiscation may apply to exclude the asset from the operation of the law by proving the lawful derivation and use of the asset (he bears the burden of proof).

Table 50: Confiscation methods in the APEC Economies

APEC Economy	Value-based	Property-based
Australia	Yes	Yes
Brunei Darussalam	Yes	Yes

Canada	Yes	Yes
Chile		
People's Republic of China	No	Yes
Hong Kong, China	Yes	Yes
Indonesia	No	Yes
Japan	Yes	Yes
Republic of Korea	Yes	Yes
Malaysia	Yes	Yes
Mexico	No	Yes
New Zealand	Yes	Yes
Papua New Guinea	Yes	Yes
Peru	No	Yes
The Philippines	Yes	Yes
Russia	Yes	Yes
Singapore	Yes	Yes
Chinese Taipei	Yes	yes
Thailand	Yes	Yes
United States	Yes	Yes
Viet Nam	No	Yes

B. Confiscation proceedings

There are different confiscation proceedings available in the APEC economies: criminal, civil proceedings, non-conviction based (NCB) –which may take place at criminal or civil Courts- and administrative confiscation. The Principles of Effective Asset Recovery adopted by the G20 Anticorruption Group recommend the implementation of a wide range of options for asset recovery, such as non-conviction based confiscation, unexplained wealth orders, and private (civil) law actions.[263]

1. Criminal Confiscation

In criminal confiscation cases, the recovery of the assets only begins after a criminal conviction, and is usually made through a final order of confiscation which is often part of the sentence. Hence, the defendant must be convicted for the offence beyond reasonable doubt. In ordering confiscation, some economies use the same standard of proof used for the conviction, while others (particularly those with a common law system) have established a lower balance of probabilities standard.[264]

Criminal confiscation is a proceeding against the person (*in personam* order). It can be object-based, which means that the prosecuting authority must prove that the assets in question are proceeds or instrumentalities of the crime, or value-based which implies allow for the forfeiture of the value of the offender's benefit from the crime.[265]

Furthermore, some jurisdictions have enacted "absconding provisions" which permit to declare the offender "convicted" for confiscation purposes once it is established that he or she has fled the jurisdiction.[266]

2. Private law actions

In some economies, such as Mexico[267] and Canada,[268] among others, the proceeds of corruption can be recovered through the initiation of civil proceedings in their domestic courts or in a foreign one (the latter may be competent if the defendant is a person living in that jurisdiction, if it is an entity incorporated or doing business in the jurisdiction; if the assets are within or have transited the jurisdiction; or if an act of corruption or money laundering was committed within the jurisdiction), where the plaintiff, as a private litigant, will have to provide direct or circumstantial evidence to establish the cause of action.[269]

Civil proceedings have many positive points that should be considered. Usually, they require a lower standard of proof than criminal ones, such as balance of probabilities. Furthermore, they can take place even in the absence of defendants.[270]

When the assets are located in a foreign economy, initiating a civil action in that economy used to be more expedient than waiting for the enforcement of a confiscation order by the foreign economy.[271]

Moreover, a number of claims and remedies exist in the civil proceedings context:

- proprietary claims for assets,
- actions in tort,

- actions based on invalidity or breach of contract, and
- illicit or unjust enrichment.[272]

However, the cost of tracing assets, the legal fees entailed in obtaining relevant court orders, the fact that they may extend over many years are some of the drawbacks of civil proceedings.[273]

3. Non-conviction Based (NCB) Forfeiture

Another type of confiscation is non-conviction based confiscation (NCB), also referred as “in rem forfeiture”, “objective confiscation” or “civil forfeiture”. Its main characteristic is that it does not need a conviction, since it is an action against the asset itself (property-based), hence proof that the asset is the proceeds or instrumentality of a crime will be required during the proceedings.[274] Consequently, there is no need to identify the owner of such property and the evidence available.[275]

It may take place within the context of a criminal proceeding or it may be a confiscation through an independent statute with a different proceeding that is often governed by the rules of civil procedure where a lower standard of proof, such as preponderance of the evidence, is required. Some economies, such as Peru, have regulated NCB forfeiture with the same standard required to obtain a criminal conviction.[276]

NCB confiscation is not available in all jurisdictions; hence, practitioners may have difficulty in obtaining MLA to assist with investigations and to enforce NCB confiscation orders.[277]

The advantages of NCB forfeiture to combating corruption, money laundering and other criminal offences is such that the UNCAC recommends its state parties to consider enacting such a form of confiscation.[278] Some APEC economies, such as Canada, Australia, Mexico, Peru and the United States have implemented this confiscation system.

Canada has a wide range of asset recovery mechanism, including NCB asset confiscation. However, due to the constitutional division of powers in Canada where property and civil rights fall under provincial jurisdiction, NCB based asset forfeiture falls primarily under provincial law and eight out of Canada’s ten provinces do have laws that permit the use of NCB confiscation orders. Federally, Canadian law provides for conviction based forfeiture with some exceptions that allow for forfeiture of property without a conviction where an accused has died or absconded. As a result and as noted in Canada’s Asset Recovery Guide, the Government of Canada cannot respond

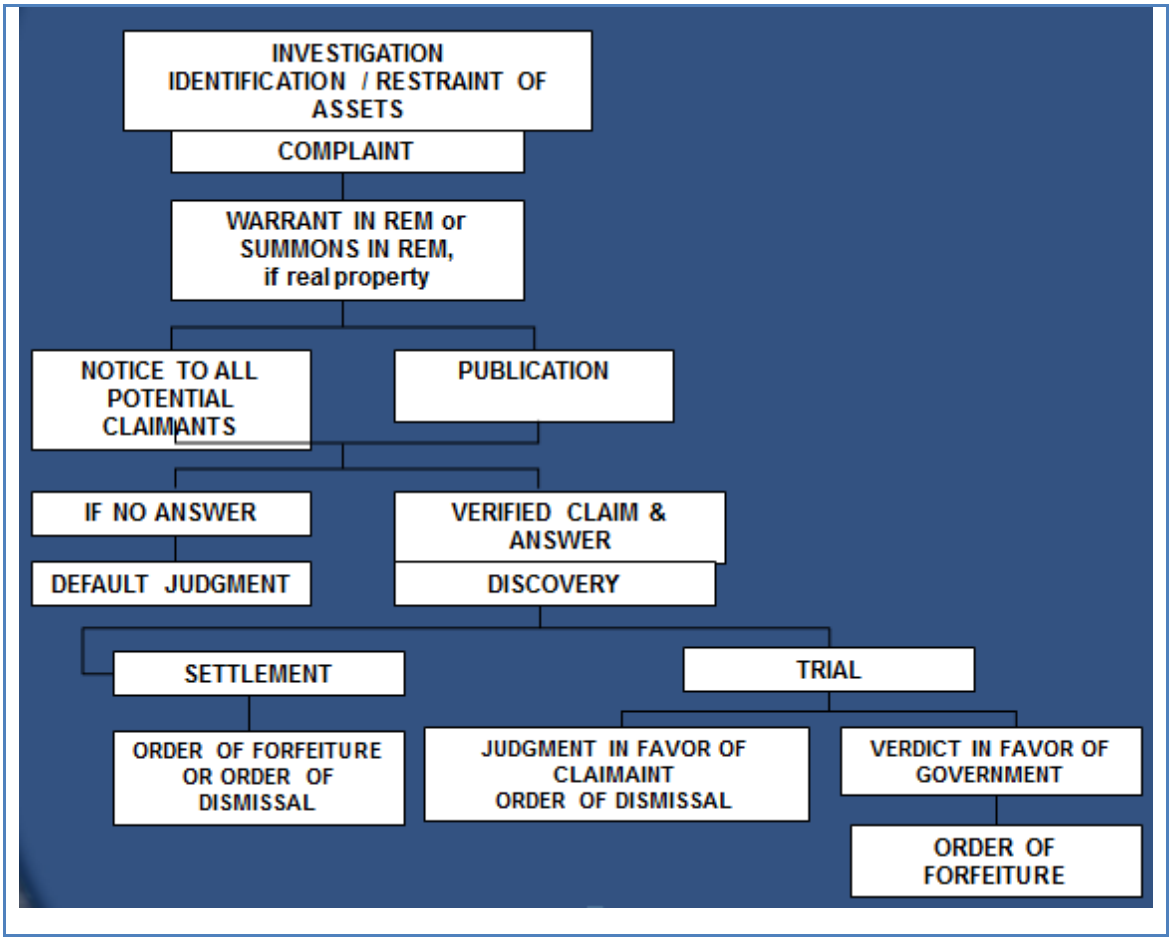
to a request for NCB asset forfeiture as such requests fall within the jurisdiction of Canada's provinces. As such, should a foreign state seek to recover assets from Canada through NCB asset forfeiture, it may convey a request to the relevant authority where the asset is located. It may also hire private counsel to act on its behalf through a civil action before the courts of that province seeking to recover the asset(s) in question.[279]

Under Article 48 of the Republic of Korea's Criminal Act, a conviction is not required for confiscation. In the absence of a conviction, what will have to be proven are the requirements listed in the provision that the thing to be confiscated was in whole or in part used or sought to be used in the commission of a crime; or is a thing produced or acquired by means of criminal conduct; or a thing exchanged for any of the preceding types of things. In addition, Korea has drafted an amendment to the Criminal Act to allow for non-conviction based forfeiture, which is to be submitted to the National Assembly, and may positively impact effectiveness in the future. Depending on the scope of the NCB, this may well enhance Korea's ability to provide requisite authority to seize and confiscate anti-corruption related assets without the need for a criminal prosecution.[280]

In Australia, NCB confiscation is allowed in all jurisdictions. There are two types of non-conviction based forfeiture order: person-directed forfeiture order and asset-directed forfeiture order. In both cases, the property must first be subject to a restraining order for at least six month before the forfeiture order can be made.[281]

Table 51: NCB Forfeiture in the United States

SOURCE: Jennifer Wallis, Trial Attorney, DOJ, U.S., PPT Presentation at the 2nd APEC Capacity-Building Workshop, September 22-24, 2014, Pattaya, Thailand.



4. Administrative Proceedings

Administrative confiscation generally involves a non-judicial mechanism for confiscating assets used or involved in the commission of the offense. Hence it does not require a judicial order by a court. It may occur by operation of statute, pursuant to procedures set out in regulations, and is typically used to address uncontested confiscation cases. The confiscation is carried out by an authorized agency (such as a police unit, customs, or a designated law enforcement agency.[282]

Generally, administrative confiscation is restricted to low-value assets or certain kinds of assets. For example, legislation may permit the confiscation of any amount of cash, but prohibit the confiscation of real property.[283] In the United States, currency of any amount and personal property valued at less than $500,000 may be administratively confiscated; but real estate, regardless of value, must always be confiscated judicially.

This type of confiscation is often associated with the enforcement of customs laws, laws combating drug trafficking, and laws requiring the reporting of cross-border transportation of currency.[284]

The advantage of this process is that it tends to be speedier and more economical than other confiscation processes.[285]

Table 52: Confiscation systems in the APEC Economies

APEC Economy	Criminal Conf.	Private law actions	NCB	Administrative
Australia	Yes	Yes	Yes. Australia's Proceeds of Crime Act 2002	-
Brunei Darussalam	Yes	No	Yes	-
Canada	Yes	Yes	Yes. Limitation: provincial law.	Yes
Chile				
People's Republic of China	Yes	Yes	No. But in the event of an action punishable by the Penalties for Administration of the Public Security Law, this type of confiscation may be conducted.	Yes.
Hong Kong, China	Yes	Yes	No. But a confiscation order may be made against an offender's criminal assets where an offender (i) has died or (ii) has absconded and the court is satisfied that reasonable steps have been taken to ascertain the person's whereabouts or to obtain the return of that person to HK, and in both circumstances, the court is	-

			satisfied that having regard to all relevant matters before it, the offender could have been convicted in respect of the offence(s) concerned.	
Indonesia	Yes	-	No	-
Japan	Yes	Yes	No (confiscation is a type of sentence).	-
Republic of Korea	Yes	Yes	Has drafted and amendment to the Criminal Act to allow NCB.	-
Malaysia	Yes	Yes	Yes	-
Mexico	Yes	Yes	No. Draft legislation.	Yes. Abandonment (in charge of the Federal Public Prosecutor)
New Zealand	Yes	Yes	Yes	-
Papua New Guinea	Yes	-	Yes	-
Peru	Yes	-	No	-
The Philippines	Yes	Yes	Yes	-
Russia	Yes	-	-	-
Singapore	Yes	Yes	No, but where an offender has absconded or deceased and the court is satisfied on the balance of probabilities that this is the case, and having regard to all the evidence before it, that such evidence if unrebutted would warrant a conviction, a confiscation order may be	-

			made.	
Chinese Taipei	Yes	No	-	-
Thailand	Yes	Yes	Yes	-
United States	Yes	Yes	Yes	Yes
Viet Nam	Yes	-	-	-

C. International Cooperation in Confiscation Proceedings

The recovery of the proceeds of corruption use to involve the cooperation with foreign jurisdictions. Sometimes, an economy needs another jurisdiction to enforce a confiscation order. This could be done through a MLA request, legally based on a multilateral o bilateral treaty or on reciprocity. The order from the requesting economy may be directly registered and enforced by the requested economy or it may be indirectly enforced through an order from a domestic court (based on facts provided by the requesting economy).[286]

In Australia, after a formal request is sent to the Attorney General to enforce a foreign forfeiture order, he/she can authorize either the Director of Public Prosecutions or Commissioner of AFP to apply for registration of the order before a court. Once registered, they are enforced as if they were made under the Proceeds of Crime Act (POCA).[287]

In Hong Kong, a mutual legal assistance (MLA) unit counsel will work with a local law enforcement officer appointed to draft the necessary application to the court for enforcement of a foreign confiscation or forfeiture order. The authority of the requesting economy should provide a certificate certifying that the confiscation order is in place and that it is final. After that, the MLA counsel will apply to the Court of First Instance to register the external confiscation order. The defendants and other affected parties will be notified and if they do not apply to the court, within a fixed period of time, to set aside the registration, the MLA counsel will apply further to enforce the foreign confiscation order, either by appointing a receiver to sell the property, or obtaining a direct payment into court when only funds in bank accounts are involved.[288]

D. Disposal of Confiscated Assets

After the assets are confiscated they have to be liquidated and the proceeds paid into a government account or general treasury. For this reason, some economies, such as Australia, Canada, Chile, Thailand and the United States, have established asset

confiscation funds into which the proceeds of the liquidated assets are to be paid. A list of economies with confiscation funds has been included below:

Table 53: Asset Forfeiture Funds

SOURCE: Greenberg, T. S., et. al., Stolen Asset Recovery—A Good Practices Guide to Non-Conviction Based Asset Forfeiture (Washington, DC: World Bank, 2009), Box 31, p. 91.

Country	Name of fund	Enabling legislation
Antigua and Barbuda	Forfeiture Fund	Money Laundering Prevention Act of 1996 (Am 2001), Section 20A
Argentina	Forfeiture Fund	Law 25.246 of 2000, Section 27
The Bahamas	Confiscated Assets Fund	Proceeds of Crime Act (2000), Section 52
Brazil	National Anti-Drug Fund (FUNAD)	Law 7560 of 1986
Canada	Seized Property Proceeds Account	Seized Property Management Act, S.C. 1993, c. 37, Section 13
Chile	National Fund for Regional Development	Act 19.366, Article 28
Colombia	Rehabilitation, Social Investment and Fight against Organized Crime Fund (FRISCO)	Law 333 of 1996, Article 25, and Law 793 of 2002, Article 12
Costa Rica	Account of the National Drug Prevention Centre	Law 7786, Article 84
Dominican Republic	Fund of the National Drugs Council	Law 50 of 1988, Article 76
Grenada	Confiscated Assets Fund	Proceeds of Crime Act 2002, Section 57
Guernsey	Seized Assets Fund—Drugs Seized Assets Fund—Proceeds of Crime	No statutory provision
Guatemala	Forfeiture Fund	Law Against Drug-Related Activities, Article 18
Haiti	Special Fund to Fight against Drugs (for crimes related to drugs and money laundering)	Control and Repression of Drug Traffick-ing, Article 88
Israel	Forfeiture Fund	Prohibition on Money Laundering Law, Section 23, applies the Dangerous Drugs Ordinance, Section 36H(a)

Table 53: Asset Forfeiture Funds (continued)

SOURCE: Greenberg, T. S., et. al., *Stolen Asset Recovery—A Good Practices Guide to Non-Conviction Based Asset Forfeiture,* 2009, Box 31, p. 91.

Luxembourg	Fund for the Fight against Drug Trafficking (Fonds de Lutte contre le Trafic Stupéfiants)	Law of 29 January 1993
Paraguay	Forfeiture Fund	Law No. 1015 of 1996, Article 37
Saint Kitts and Nevis	Forfeiture Fund	Proceeds of Crime Act (2000), Section 61
Saint Vincent and the Grenadines	Seized Assets Fund	Proceeds of Crime Act (2000), Section 58
South Africa	Criminal Assets Recovery Account (for both criminal and NCB asset forfeiture)	Prevention of Organised Crime Act (Am) 1998, Section 63
Switzerland	No national fund; fund in Geneva (for narcotics offenses)	
Thailand	Anti-Money Laundering Fund	Anti-Money Laundering Act 1999 (Am No. 2 2008)
Trinidad and Tobago	Seized Assets Fund	Act 55 of 2000, Section 58
Turks and Caicos	Forfeiture Fund	Proceeds of Crime Ordinance of 1998 (2007 Am)
United Kingdom	An asset forfeiture scheme No statutory provision	
United States	Department of Justice Assets Forfeiture Fund	Title 28 United States Code Section 524(c)

Countries that do not have a fund: Mexico, Liechtenstein, Nigeria, the Philippines. Rather than a forfeiture fund, the Government of Mexico distributes the forfeited funds, in equal shares, to the ministries responsible for health, law enforcement, and the judiciary.

E. Recovery measures beyond confiscation

Apart from confiscation, there are other measures used by the APEC Economies as sanctions in corruption or money laundering cases intended to recover the proceeds of crime.

One of those measures is the imposition of monetary fines. Whether criminally or civilly established, they are designed to punish misconduct and deter future offences by a

defendant and others. For example, in Australia the maximum fine for an individual for foreign bribery is U$s 1.1 million and for an enterprise U$s 11 million.[289] In the U.S., criminal penalties under the FCPA include a fine of up to U$s 2,000,000 for corporations, and a fine of up to U$s 250,000, and under the Alternative Fines Act, these fines may be higher –the actual fine may be up to twice the benefit that the defendant sought to obtain by making the corrupt payment–.[290]

Another measure, used mainly in the United States in –among others- foreign bribery cases by the Securities Exchange (SEC) Commission, is known as disgorgement of profits. The Securities Exchange Act of 1934 authorized this remedy as part of administrative or cease and desist proceedings, which is used to –civilly- deprive wrongdoers of their ill-gotten gains, meaning that the wrongdoer is required to give up any (net) profits he made as a result of his illegal conduct.[291]

Disgorgement of profits is an equitable remedy intended as a vehicle for preventing unjust enrichment, rather than as a tool to punish. Hence, under disgorgement (or similar unjust enrichment measures) authorities can only recover the approximate amount earned from the alleged wrongful activities (otherwise, it will be considered a sanction).[292]

When calculating disgorgement, authorities have to distinguish between legally and illegally obtained profits. First, it is necessary to identify the causal link between the illegal activity and the profit to be disgorged. Afterwards, if the causal link is established, profits from the illegal activity may be disgorged. In the United States, the SEC has considerable discretion to determine what constitutes illicit profits. Courts have recognized this, and require only a "reasonable approximation of the profits which are causally connected to the violation"[293]. Then, the burden shifts to the defendant, who must rebut the causal connection.

The first case in which the SEC ordered this remedy was in 2004, when ABB Ltd disgorged $5.9 million to settle civil anti-bribery, books-and-records, and internal-controls offenses. Since then the SEC has used disgorgement in about three-quarters of its FCPA-related enforcement actions.

Table 54: Disgorgement in Corporate SEC Dispositions

SOURCE: Sasha Kalb and Marc Alain Bohn, "Disgorgement: The Devil You Don't Know", *Corporate Compliance Insights*, available in:

http://www.corporatecomplianceinsights.com/disgorgement-fcpa-how-applied-calculated/

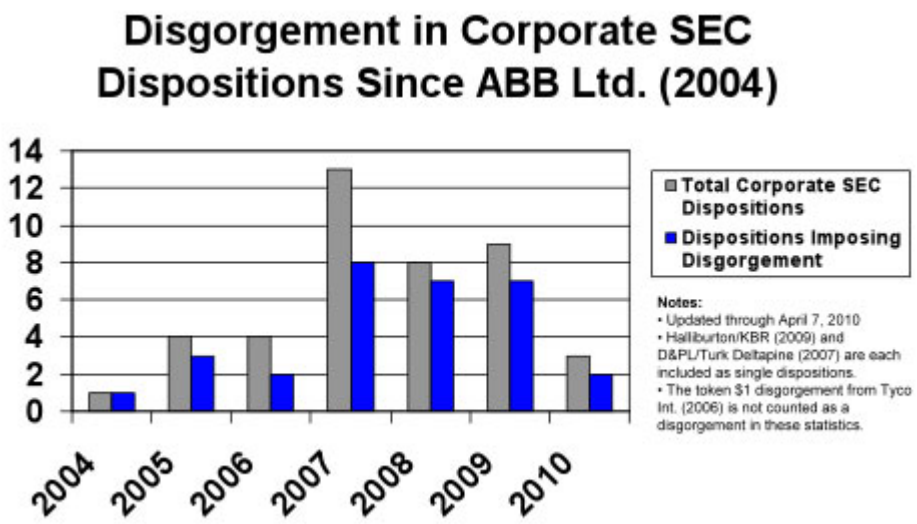


Table 55: Top eleven FCPA-related corporate disgorgements

Source: http://www.fcpablog.com/blog/2014/12/26/avon-disgorgement-lands-on-top-ten-list.html (last visited 26 August, 2015)

1. Siemens U$s 350 million (2008)
2. KBR U$s 177 million (2009)
3. Alcoa U$s 161 million (2014)
4. Total S.A. U$s 153 million (2013)
5. Snamprogetti U$s 125 million (2010)
6. Technip U$s 98 million (2010)
7. Daimler U$s 91.4 million (2010)

8. Avon U$s 67.35 million (2014)

9. Pfizer U$s 45.2 million (2012)

10. Alcatel-Lucent U$s 45 million (2010)

CHAPTER X. REPATRIATION OF CONFISCATED ASSETS TO THE MEMBER ECONOMY OF ORIGIN

Repatriation is the process through which the confiscated property returns to its prior legitimate owner.[294] There is universal agreement to the principle that confiscated funds originating from corruption should be returned to its legitimate owner. In fact, it is established in the United Nations Convention against Corruption (UNCAC) as a fundamental principle of the Convention.[295] Furthermore, UNCAC stresses that each party to the Convention shall adopt legislative and other measures as may be necessary to enable its competent authorities to return confiscated property when it's requested by another party,[296] and foresees that, where appropriate, they may conclude agreements for the final disposal of the confiscated assets.

A. Asset Return

Although there is consensus among the APEC economies about the necessity to return stolen confiscated assets to its prior legitimate owner, today there is no standard procedure for returning those assets; article 57 of UNCAC does not settle that procedure. Hence, it is a process driven by pragmatic considerations which depends on a case-by-case basis and on whether there are specific arrangements in force.[297]

Once the proceedings to recover stolen assets are successfully completed and the illegal assets are confiscated, the question of their restitution arises.[298] A requesting economy may apply for the return of assets to enforce a decision of its own courts or whilst criminal investigations or proceedings are still pending. In the first situation, the transfer of assets will only take place if and when a final and binding decision ordering the confiscation of the relevant assets or their restitution to legitimate claimants is issued by the courts of the requesting economy.[299] Most economies require a criminal conviction in the requesting jurisdiction prior to repatriating the assets.[300] In the second situation, the return of property to the requesting economy may be permissible at any stage of the foreign proceedings and prior to the issuance of a judicial decision;[301] this is not common practice among the APEC economies.

UNCAC establishes that in cases of embezzlement of public funds or of laundering of embezzled public funds the requested party shall return the confiscated property to the requesting party, when the assets were confiscated by the requested party on the basis of a final judgment in the requesting party. In cases of any other corruption-related offences the requested party will have to return the confiscated property to the

requesting party, when the latter reasonably establishes its prior ownership of such confiscated property or when the requested party recognizes damage to the requesting one as a basis for returning the confiscated property.[302]

Another aspect that needs to be considered when analyzing the return of assets is who the legitimate owner of the stolen assets is. In cases of corruption and misappropriation of public funds, the prior legitimate owner would be the economy from which such funds have been stolen (after considering the rights of *bona fide* third parties and the expenses incurred by the foreign economy)[303].

Furthermore, how the assets will be returned or whether they will be returned in whole or in part to the requested jurisdiction is another issue of concern among the economies, since the MLA legislation of most APEC economies is either silent or vague on this issue, and the MLA treaties in force generally give the requested jurisdiction wide discretion in dealing with confiscated assets (some MLA treaties such as the Australia-Hong Kong, China, the Hong Kong, China-Singapore, the India-Thailand, the Korea-Philippines and Korea-Vietnam treaties stipulate that the requested economy will retain confiscated proceeds of crime unless the parties decide otherwise; others such as the Australia-Malaysia, the P.R. China-Korea or the Korea-Thailand treaties state that forfeited proceeds may be transferred to the requesting jurisdiction, subject to the applicable domestic law and agreement between the parties).[304]

Nonetheless, there are some MLA treaties that contain specific obligations related to the return of confiscated assets, such as the Australia-Indonesia, the Australia-Philippines and the P. R. China-Indonesia treaties which mandate repatriation of confiscated assets or their value, or the Hong Kong, China-Philippines treaty which explicitly obliges the requested economy to execute a final decision by a court of the requesting economy that imposes confiscation and to return the property or the proceeds to the requesting economy.[305]

Table 56: The legislation related to return of confiscated assets of some APEC economies

SOURCE: ADB/OECD Anti-Corruption Initiative for Asia and the Pacific, *Mutual Legal Assistance, Extradition and Recovery of proceeds of Corruption in Asia and The Pacific*, 2007, pp. 86-87.

Australia	Property subject to a registered foreign forfeiture order may be disposed of or otherwise dealt with in accordance with any direction of the Attorney-General, which may include giving all or part of the assets to the requesting economy.
Hong-Kong, China	The Secretary of Justice has discretion to give all or part of the confiscated assets to the requesting economy that is a treaty partner.
Malaysia	The government has absolute discretion to manage and dispose of the seized property.
Indonesia	Legislation requires entering into an agreement with the requesting economy for reciprocal sharing of the proceeds of confiscated assets that have been auctioned.
Japan	Repatriation of assets to another economy on a case-by-case basis and upon an assurance of reciprocity by the requesting economy.
Thailand	The forfeited assets become Thailand's property.

Even when the economy is willing to repatriate the assets to its prior legitimate owner, it may impose certain conditions on how and when to use or distribute the assets. One option that has been reviewed by international financial institutions is the use of the assets for the partial settlement of debts at a bilateral or multilateral level. However, the allocation of assets to public debt relief requires an in-depth review of both technical feasibility and its political suitability, keeping in mind the perception that the reduction of public debt might not benefit the general population.[306] Another option was used by

Switzerland in a case involving the proceeds of corruption originating from Nigeria, when it transferred the assets to the Bank for International Settlements, most of which were later spent on housing projects, education and allocations to state governments in Nigeria.[307]

It is widely recognized that the recovery and return of stolen assets could provide essential resources for the financing of public services and investments in infrastructure and other programs aimed at social and economic development. However, the economies may have legitimate concerns regarding repatriating confiscated assets to countries where corruption levels remain high and governance is weak, since they may fear that the returned assets could be poorly managed or simply embezzled again. Different solutions have been proposed to address that concern, such as the monitoring of assets.

B. The Monitoring of Assets

Another concern among the economies is the lack of a treaty-based mechanism allowing for the allocation or the monitoring of the returned assets, to ensure that they are used to create development funds or for like purposes at the victim jurisdiction.

Monitoring refers to different forms and degrees of control and supervision of the use of restituted funds in the recipient economy. At the end of the scale, monitoring includes 'ring-fencing' by channeling the funds through vehicles that are independent of government, such as trust funds, foundations, or dedicated public accounts (or escrow accounts). Such arrangements could even include a step-by-step restitution, subject to certain tranche release conditions. At the other end of the scale, monitoring could simply be a review of the management of the budget in cases where restituted funds flow into the general government budget. What is common in most cases, however, is an element of external review, either in the form of the disclosure of the results of monitoring, or the active participation of third parties, such as international organizations and/or civil society organizations, in the process.[308]

UNCAC allows the parties to conclude agreements or mutually acceptable arrangements for the disposal of confiscated property. Such agreements are concluded regularly. One remarkable example is the transfer of the funds, which were intended as bribes for Kazakh officials, to be used by a foundation supervised by the World Bank to help poor children in Kazakhstan.

For a comprehensive understanding of the monitoring of returned assets, we will analyze the relevant cases regarding the subject.

Table 57: Cases of monitoring of returned assets

SOURCE: ATTISSO, K., and FENNER ZINKERNAGEL, G., "Past experience in agreements for the disposal of confiscated assets", *Emerging trends in asset recovery*, 2013, pp. 336-340.

The Abacha Case - External ex-post monitoring

General Sani Abacha, Minister of Defense and Chief on Army Staff of Nigeria, took power through a *coup d'etat*. Corrupt practices became blatant and systematic. Funds were removed in cash from the Central Bank, sometimes by the truck-load, and taken out of the economy by members of the Abacha family and their associates. Inflated public contracts were also awarded to members of the Abacha family and/or their associates. The 'Abacha loot' was in Swiss banks until its repatriation.

Following long negotiations, Nigeria and Switzerland agreed that the Abacha's stolen assets were going to be used in projects aimed to benefit Nigerian poor people under the supervision of a third party, the World Bank, through Integrity, a Nigerian civil society organization. Integrity, together with other local civil society organizations, reviewed 51 projects.

The greatest challenge encountered was related to the appropriation and tracking of funds in the national budget. There were several instances in which spending agencies used the Abacha loot either to defray out-standing arrears or to make partial payments for ongoing multi-year projects. The actual implementation of the projects funded by the Abacha loot was affected by problems of inefficiency, lack of good faith and corruption. The findings of the World Bank review were also mixed. They showed that implementation for all projects had commenced and that most had been completed. However, the quality and impact of projects varied greatly across sectors and significant weaknesses in budget accounting and reporting were identified.

In conclusion, appropriate budget coding for tracking the use of resources is crucial to demonstrate the developmental impact of asset recovery and to make sure that a maximal part of the population profits from the restitution. The difficulties experienced show also that ex-post facto monitoring mechanisms are of limited use and that systems should be set-up to enable a continuous monitoring.

The Vladimiro Montesinos case - National Monitoring

Vladimiro Montesinos was head of Peru's secret service and advisor to President Alberto Fujimori between 1990 and 2000. In 2000 secret videos were televised showing Montesinos bribing the opposition. Subsequent investigations revealed multi-million dollar dealing in illegal activities, including extortion of high profile entrepreneurs, embezzlement, graft, dealings in the arms trade and drug trafficking. Since his conviction, Peru has recovered over USD 185 million.

In October 2001, Peru created the *Fondo de Administración del Dinero Obtenido Ilícitamente en perjuicio del Estado* (FEDADOI) (Special Fund of Management of Illegally Obtained Money Against Interests of the State), by emergency decree 122-

2001. The repatriated assets were channeled into this special fund managed by a board of five members appointed from different government ministries.

Although guidelines and detailed procedures were defined to ensure the transparent use of the recovered assets, money in the fund has so far ended up supplementing the annual fiscal budget of agencies that had a member on the FEDADOI board. Other monies were used to finance leisure activities for the police.

The Kazakhstan case: BOTA Foundation - Trilateral monitoring

A 1999 case involving a US citizen investigated under the US Foreign Corrupt Practices Act uncovered corrupt payment to Kazakh officials amounting to USD 84 million that was paid into a Swiss bank.

The payments were made on behalf of US oil companies, including Mobil Oil Corp, to obtain concessions to exploit oil resources. The BOTA (meaning young camel in Kasak) is an independent non-profit foundation established in May 2008 following the 2007 trilateral agreement between the governments of the Republic of Kazakhstan, the United States of America and the Swiss Confederation to channel the recovered funds into projects that benefit disadvantaged children in Kazakhstan.

The evaluations of the BOTA program conducted over the last two years by Oxford Policy Management (OPM) at the request of the concerned parties also confirmed that the implementation of the program across all activities was highly effective for the beneficiaries. On the other hand, the administrative costs of the arrangement are extremely high and may end up amounting to one third of the total funds returned to Kazakhstan.

The Angola case - Monitoring by a bilateral development agency

Switzerland confiscated assets as part of a domestic criminal investigation in Geneva in April 2002, which related to the diversion of Angolan oil revenues supposedly destined to repay the economy's debt with Russia. While proceedings were suspended in 2004 after the investigation found no irregularities, a total of USD 21 million held in accounts under the names of four high-ranking Angolan public officials remained frozen as the concerned individuals had not disputed that the money actually belonged to the Angolan State. In 2005, the Angolan and the Swiss authorities signed an agreement.

The assets were to be used for social and humanitarian purposes the Swiss Agency for Development Cooperation (SDC) were to administer the funds and provide support to the program. Angola was named as the beneficial owner but only SDC was authorized to initiate the withdrawal of funds.

In 2012, in a second case, Switzerland and Angola signed another agreement over the repatriation of about USD 43 million. The funds are again administered by SDC as per the earlier arrangement, and they benefit similar purposes.

Some Swiss NGOs criticized the use of part of the confiscated assets for a contract

with the Swiss company RUAG, as it was perceived as not transparent and reminiscent of the old tied aid principles. Given that this arrangement was chosen at the request of the Angolan government, however, it would seem an adequate choice. This case illustrates some of the risks associated with channeling funds back through bilateral aid programs, as the requested State may be exposed to potential criticism.

REFERENCES

[1] Further information regarding this workshop, including the agenda and presentations are available at http://www.fiscaliadechile.cl/apecactworkshopchile/index.html

[2] UNODC (United Nations Office on Drugs and Crime) (2004), *Practical Anti-Corruption Measures for Prosecutors and Investigators,* Vienna, Austria, p. 44, available at: www.unodc.org/pdf/crime/corruption/Handbook.pdf

[3] FATF, *Operational Issues. Financial Investigation Guidance*, June 2012, p. 8

[4] FATF, *Operational Issues. Financial Investigation Guidance*, June 2012, p. 29

[5] USAID Nepal, *Anticorruption Investigation and Trial Guide: Tools and Techniques to Investigate and Try the Corruption Case*, August 2005, p. 7-8, available at http://pdf.usaid.gov/pdf_docs/PNADE146.pdf. The gathering of evidence will be treated with more detail in the following Sections.

[6] *Reactive detection* takes place where a formal complaint –either from individuals, governmental agencies, or private companies, among others– is received by the law enforcement agency, forming the basis for investigation. Where the complaint comes from a governmental agency, it may be based on information derived from disclosure and reporting requirements as well as audits and inspections. Instead of complaint-based, *pro-active detection* is intelligence-based. It takes place, e.g., after law enforcement agencies conducted an undercover investigation pursuing intelligence information.

[7] UNODC (United Nations Office on Drugs and Crime) (2004), *Practical Anti-Corruption Measures for Prosecutors and Investigators,* Vienna, Austria, p. 36-38, available at: www.unodc.org/pdf/crime/corruption/Handbook.pdf

[8] For instance, when during the course of an integrity test the corrupt tendencies of an official may have been established, meaning that no further investigation is necessary.

[9] UNODC (United Nations Office on Drugs and Crime) (2004), *Practical Anti-Corruption Measures for Prosecutors and Investigators,* Vienna, Austria, p. 38, available at: www.unodc.org/pdf/crime/corruption/Handbook.pdf

[10] Ibid.

[11] UNODC, The Global Programme Against Corruption: UN Anti-Corruption Toolkit, 3nd Edition, Vienna, September 2004

[12] Recommendation Rec(2005)10 of the Committee of Ministers of the Council of Europe to members on “special investigation techniques” in relation to serious crimes including acts of terrorism.

[13] FATF, *Operational Issues. Financial Investigation Guidance*, June 2012, p. 26-27, OECD, *Investigation and Prosecution of Corruption Offences: Materials for the Training Course*, Ukraine, 2012, p. 23-24

[14] FATF, *Operational Issues. Financial Investigation Guidance*, June 2012, p. 11; UNODC (United Nations Office on Drugs and Crime) (2004), *Practical Anti-Corruption Measures for Prosecutors and Investigators,* Vienna, Austria, p. 54, available at: www.unodc.org/pdf/crime/corruption/Handbook.pdf

[15] http://www.egmontgroup.org/about/financial-intelligence-units-fius.

[16] Conf. FATF Recommendation 31, available at: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

[17] FATF, *Operational Issues. Financial Investigation Guidance*, June 2012, p. 22.

[18] Article 48 of the UNCAC encourages law enforcement authorities in different jurisdictions to strengthen their co-operation in order to enhance the effectiveness of law enforcement action to combat corruption, through for example, the exchange of information and co-ordination of administrative actions for the purpose of early identification of the offence, as well as exchange of personnel and liaison officers.

[19] FATF, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. The FATF Recommendations*, February 2012, Recommendation 32, p. 25, available at: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

[20] STAR (Stolen Asset Recovery) Initiative, The World Bank, UNODC, Barriers to Asset Recovery, Washington DC., 2011, p. 43, at http://www.unodc.org/unodc/en/corruption/StAR.html.

[21] FATF paper, best practices on confiscation (FATF 2010), available at: http://www.coe.int/t/dghl/monitoring/moneyval/web_ressources/FATF_BPR3&38.pdf

[22] Informal Expert Working Group on Effective Extradition Casework Best Practice (UNODC), Report. Vienna, 2004, p. 12, at http://www.unodc.org/documents/legal-tools/lap_report_ewg_extradition_casework.pdf.

[23] See *infra*.

[24] UNODC (United Nations Office on Drugs and Crime), Manual on Mutual Legal Assistance and Extradition, New York, 2012, p. 68, at http://www.unodc.org/documents/organized-crime/Publications/Mutual_Legal_Assistance_Ebook_E.pdf.

[25] It is increasingly recognized that joint investigation teams (JITs) is an effective form of international co-operation in investigation and prosecution of trans-border corruption cases involving several economies.

[26] All APEC economies except for Hong Kong and Chinese Taipei are members of Interpol.

[27] See, http://www.interpol.int/About-INTERPOL/Overview.

[28] See, http://www.egmontgroup.org/.

[29] The FIUs of the following APEC economies are members of the Egmont Group: Australia, Canada, Chile, Hong Kong, China, Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Peru, The Philippines, Russia, Singapore, Chinese Taipei, Thailand and The United States.

[30] ACPO, *Practice Advice On Financial Investigation*, p. 28.

[31] The process is based on the model developed in *ACPO (2005) Practice Advice on Core Investigative Doctrine*

[32] FATF, *Operational Issues. Financial Investigation Guidance*, p. 17.

[33] FATF, *Operational Issues. Financial Investigation Guidance*, p. 17.

[34]See www.cicad.oas.org/Lavado_Activos/ENG/Documents/Information%20Sources%20Exchange_Eng.doc.

[35] Association of Chief Police Officers (ACPO), *Practice Advice On Financial Investigation*, 2006

[36] US OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, *Intelligence Community Directive*, Number 301. National Open Source Enterprise. Section F(3), July 11, 2006.

[37] EHREN, Colin, "Challenges of Gathering Evidence from the Internet", presented at the APEC Anti-Corruption and Transparency Working Group (ACTWG), *Capacity Building Workshops on Designing Best Models on Prosecuting Corruption and Money Laundering Cases Using Financial Flow Tracking Techniques and Investigative Intelligence for Effective Conviction and Asset Recovery to Promote Regional Economic Integration*, Santiago, Chile, 11-13 June 2013.

[38] US GAO, *Investigators' Guide to Sources of Information*, OSI-97-2, Apr 1, 1997, at www.gao.gov/products/OSI-97-2

[39] U.S. GAO*, SOCIAL MEDIA. Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate*, GAO-11-605, June 28, 2011, at www.gao.gov/products/GAO-11-605

[40] U.S. GAO*, SOCIAL MEDIA. Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate*, GAO-11-605, 2011.

[41] D. L. CARTER, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, Second Edition, Office of Community Oriented Policing Services - U. S. Department of Justice, Washington, 2009, p. 283.

[42] D. L. CARTER, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, Second Edition, Office of Community Oriented Policing Services - U. S. Department of Justice, Washington, 2009, p. 283.

[43] D. L. CARTER, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, Second Edition, Office of Community Oriented Policing Services - U. S. Department of Justice, Washington, 2009, p.290.

[44] D. L. CARTER, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, Second Edition, Office of Community Oriented Policing Services - U. S. Department of Justice, Washington, 2009, p.290.

[45] H.MULUKUTLA – M. RÜEGG, *The Importance of Information Technology in Tracing Stolen Assets*, in INTERNATIONAL CENTRE FOR ASSET RECOVERY, *Tracing Stolen Assets: A Practitioner's Handbook*, Basel Institute on Governance, Basel, 2009, p. 79

[46] BACARESE, *The Role of Intelligence in the Investigation and the Tracing of Stolen Assets in Complex Economic Crime and Corruption Cases*, p. 46. See National Commission on Terrorist Attacks Upon the United States. (2004). The 9/11 Commission Report. Washington, DC: U.S. Government Printing Office, 413.

[47] BACARESE, *The Role of Intelligence in the Investigation and the Tracing of Stolen Assets in Complex Economic Crime and Corruption Cases*, p. 46.

[48] See D. L. CARTER, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, Second Edition, Office of Community Oriented Policing Services - U. S. Department of Justice, Washington, 2009, p.285.

[49] BACARESE, *The Role of Intelligence in the Investigation and the Tracing of Stolen Assets in Complex Economic Crime and Corruption Cases*, p. 46.

[50] BACARESE, *The Role of Intelligence in the Investigation and the Tracing of Stolen Assets in Complex Economic Crime and Corruption Cases*, p. 47.

[51] BACARESE, *The Role of Intelligence in the Investigation and the Tracing of Stolen Assets in Complex Economic Crime and Corruption Cases*, p. 47.

[52] D. L. CARTER, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, Second Edition, Office of Community Oriented Policing Services - U. S. Department of Justice, Washington, 2009, p. 291.

[53] M. K. Bergman, "The Deep Web: Surfacing Hidden Value", cited by David Hunter & Karen Brown, T*hriving or Surviving*? National Library of Scotland in 2030, National Library of Scotland, 2010, pp. 39/40.

[54] D. L. CARTER, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, Second Edition, Office of Community Oriented Policing Services - U. S. Department of Justice, Washington, 2009, p. 303.

[55] D. L. CARTER, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, Second Edition, Office of Community Oriented Policing Services - U. S. Department of Justice, Washington, 2009, p. 303.

[56] D. L. CARTER, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, Second Edition, Office of Community Oriented Policing Services - U. S. Department of Justice, Washington, 2009, p. 293.

[57] IACP NATIONAL LAW ENFORCEMENT POLICY CENTER, *Social Media, Concepts and Issues Paper*, September 2010, at www.iacpsocialmedia.org/Portals/1/documents/social%20media%20paper.pdf;

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE, *Social Media Fact Sheet,* 2013, at www.iacpsocialmedia.org/Portals/1/documents/Fact%20Sheets/Social%20Media%20Fact%20Sheet.pdf

[58] COPS, *Social Media and Tactical Considerations For Law Enforcement*, May 2013, at www.iacpsocialmedia.org/Portals/1/documents/External/SocialMediaandTacticalConsiderationsforLawEnforcement.pdf

[59] See IACP CENTER FOR SOCIAL MEDIA, *2011 Survey Results*, at www.iacpsocialmedia.org/Resources/Publications/2011SurveyResults.aspx.

[60] LEXISNEXIS RISK SOLUTIONS, *Survey of Law Enforcement Personnel and Their Use of Social Media in Investigations*, 2012, at www.lexisnexis.com/investigations.

[61] IACP NATIONAL LAW ENFORCEMENT POLICY CENTER, *Social Media, Concepts and Issues Paper*, September 2010, p.1.

[62] D. L. CARTER, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, Second Edition, Office of Community Oriented Policing Services - U. S. Department of Justice, Washington, 2009, p. 290.

[63] INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE, *Social Media Fact Sheet,* 2013.

[64] U.S. GAO*, SOCIAL MEDIA Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate*, 2011.

[65] See *Facebook Newsroom* at http://newsroom.fb.com/company-info/.

[66] U.S. GAO*, SOCIAL MEDIA Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate*, 2011.

[67] See *Twitter Company Facts* at https://about.twitter.com/company.

[68] U.S. GAO*, SOCIAL MEDIA Federal Agencies Need Policies and Procedures for Managing and Protecting Information They Access and Disseminate*, 2011.

[69] V. M. KEENAN et al., *Developing Policy on Using Social Media for Intelligence and Investigations*, in *The Police Chief* 80 (June 2013): 28–30.

[70] EHREN, Colin, "Challenges of Gathering Evidence from the Internet", presented at the APEC Anti-Corruption and Transparency Working Group (ACTWG), *Capacity Building Workshops on Designing Best Models on Prosecuting Corruption and Money Laundering Cases Using Financial Flow Tracking Techniques and Investigative Intelligence for Effective Conviction and Asset Recovery to Promote Regional Economic Integration*, Santiago, Chile, 11-13 June 2013.

[71] COPS, *Social Media and Tactical Considerations For Law Enforcement*, at www.iacpsocialmedia.org/Portals/1/documents/External/SocialMediaandTacticalConsiderationsforLawEnforcement.pdf

[72] V. M. KEENAN et al., *Developing Policy on Using Social Media for Intelligence and Investigations*, in *The Police Chief* 80 (June 2013): 28–30.

[73] EHREN, Colin, "Challenges of Gathering Evidence from the Internet", presented at the APEC Anti-Corruption and Transparency Working Group (ACTWG), *Capacity Building Workshops on Designing Best Models on Prosecuting Corruption and Money Laundering Cases Using Financial Flow Tracking Techniques and Investigative Intelligence for Effective Conviction and Asset Recovery to Promote Regional Economic Integration*, Santiago, Chile, 11-13 June 2013.

[74] V. M. KEENAN et al., *Developing Policy on Using Social Media for Intelligence and Investigations*, in *The Police Chief* 80 (June 2013): 28–30.

[75] U.S. v. Joshua Meregildo et al., 11 Cr. 576 (WHP), August 10, 2012, at www.x1discovery.com/download/US_v_Meregildo.pdf.

[76] In the US, see for example, US GAO, *Investigators' Guide to Sources of Information*, OSI-97-2, Apr 1, 1997

[77] Based on US DEPARTMENT OF JUSTICE, *Financial Investigations Checklist*, at www.justice.gov/criminal/afmls/pubs/pdf/fininvguide.pdf.

[78] L. DANIEL – L. DANIEL, *Digital Forensics for Legal Professionals: Understanding Digital Evidence From The Warrant To The Courtroom*, Waltham, 2012, p. 3.

[79] J. KRAUSE, *Discovery Channels*, ABA Journal, July 2002, p. 50.

[80] J. LARUE et al., *Trails from the Aether: Cyber-Evidence*, in 54.1 State Bar of Texas 33rd Annual Advanced Family Law Course 1, 1 (2007), at www.texasbarcle.com/Materials/Events/6367/110331_01.pdf.; quoting D. BISHOP and A. HOROWITZ, *Electronic Discovery*, *Advanced Business & Commercial Litigation Course*, State Bar of Texas 2001, p. 1.

[81] S. L. HARRINGTON, *Contemporary Issues in Cyberlaw: Collaborating With a Digital Forensics Expert: Ultimate Tag-Team or Disastrous Duo?*, in *William Mitchell Law Review*, 2011, 38, 353, quoting W. E. MOOZ, Jr., *Technology Tips for Reducing EDD Review Costs*, 24 Legal Tech News, no. 12, March 2007, 1.

[82] THE RADICATI GROUP, *Email Statistics Report*, *2015-2019 Executive Summary*, at http://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf.

[83] L. DANIEL – L. DANIEL, *Digital Forensics for Legal Professionals*, p. 3.

[84] MULUKUTLA – RÜEGG, *The Importance of Information Technology in Tracing Stolen Assets*, p. 78.

[85] MULUKUTLA – RÜEGG, *The Importance of Information Technology in Tracing Stolen Assets*, p. 78.

[86] S. L. HARRINGTON, *Contemporary Issues in Cyberlaw: Collaborating With a Digital Forensics Expert,* p. 355.

[87] The following boxes are an adaptation from DANIEL – DANIEL, *Digital Forensics for Legal Professionals*, p. 11 ff.

[88] NATIONAL INSTITUTE OF JUSTICE, *Electronic Crime Scene Investigation: A Guide for First Responders*, April 2008, Washington, p. vii.

[89] The presented protocols and procedures largely represent an adaptation of guidance published in NATIONAL INSTITUTE OF JUSTICE, *Electronic Crime Scene Investigation: A Guide for First Responders*, p. 15 ff.; DANIEL – DANIEL, *Digital Forensics for Legal Professionals*, p. 25 ff.; SCIENTIFIC WORKING GROUP ON DIGITAL EVIDENCE, *Best Practices for Computer Forensic 2014*, at https://www.swgde.org/documents/Current%20Documents/2014-09-05%20SWGDE%20Best%20Practices%20for%20Computer%20Forensics%20V3-1.

[90] DANIEL – DANIEL, *Digital Forensics for Legal Professionals*, p. 28.

[91] NATIONAL INSTITUTE OF JUSTICE, *Electronic Crime Scene Investigation: A Guide for First Responders*, p. 21.

[92] See J. E. FELDMAN, *The Basics of Computer Forensics*, p. 20, in *The Practical Litigator*, March 2001, 17.

[93] S. D. NELSON - B. A. OLSON - J. W. SIMEK, *The Electronic Evidence and Discovery Handbook*, American Bar Association, 2006, p. 259. The definition is also contained in the US Code of Federal Regulations (§1234.2).

[94] See DANIEL – DANIEL, *Digital Forensics for Legal Professionals*, p. 240 ff.

[95] See DANIEL – DANIEL, *Digital Forensics for Legal Professionals*, p. 36.

[96] See the SOCA *National intelligence requirement for serious organised crime*, 2008-9, as cited in A. BACARESE, *The Role of Intelligence in the Investigation and the Tracing of Stolen Assets in Complex Economic Crime and Corruption Cases*, in INTERNATIONAL CENTRE FOR ASSET RECOVERY, *Tracing Stolen Assets: A Practitioner's Handbook*, Basel Institute on Governance, Basel, 2009, p. 39-40.

[97] Examples are taken from LASICH, *The Investigative Process – a Practical Approach*, p. 56 ff.

[98] BACARESE, *The Role of Intelligence in the Investigation and the Tracing of Stolen Assets in Complex Economic Crime and Corruption Cases*, p. 45.

[99] BACARESE, *The Role of Intelligence in the Investigation and the Tracing of Stolen Assets in Complex Economic Crime and Corruption Cases*, p. 45.

[100] USAID, *Anticorruption Investigation and Trial Guide: Tools and Techniques to Investigate and Try the Corruption Case*, August 2005, at pdf.usaid.gov/pdf_docs/PNADE146.pdf

[101] USAID, *Anticorruption Investigation and Trial Guide*, p. 6 ff.

[102] ATKINSON P., "Asset tracing", in *Emerging trends in Asset Recovery*, p. 220.

[103] ATKINSON P., "Asset tracing", in *Emerging trends in Asset Recovery*, p. 220.

[104] Nine Key Principles of Effective Asset Recovery Adopted by the G20 Anticorruption Working Group, Cannes, 2011, available at: http://StAR.worldbank.org/StAR/sites/StAR/files/asset_recovery_country_profiles.pdf.

[105] FATF, *Operational Issues. Financial Investigation Guidance*, June 2012, p. 3, available at: http://www.fatf-gafi.org/media/fatf/documents/reports/Operational%20Issues_Financial%20investigations%20Guidance.pdf.

[106] The FATF Recommendations, February 2012, available at: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf.

See Interpretive Note to Recommendation 30 (Responsibilities of Law Enforcement

and Investigative Authorities), p.97, para. 2.

[107] FATF, *Operational Issues. Financial Investigation Guidance*, p. 3, para. 2.

[108] USAID Nepal, Anticorruption Investigation and Trial Guide: Tools and Techniques to Investigate and Try the Corruption Case, August 2005, p. 28, available at: http://pdf.usaid.gov/pdf_docs/PNADE146.pdf.

[109] OECD, Investigation and Prosecution of Corruption Offences: Materials for the Training Course, Ukraine, 2012, p. 7, available at: http://www.oecd.org/corruption/acn/lawenforcement/TrainingManualcorruptionoffences2012EN.pdf.

[110] OECD, Investigation and Prosecution of Corruption Offences: Materials for the Training Course, Ukraine, 2012, p. 8, available at: http://www.oecd.org/corruption/acn/lawenforcement/TrainingManualcorruptionoffences2012EN.pdf.

[111] StAR (Stolen Asset Recovery) Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 58, available at: https://StAR.worldbank.org/StAR/sites/StAR/files/Asset%20Recovery%20Handbook.pdf.

[112] ACPO (Association of Chief Police Officers, UK), Centrex, Practice Advice on Financial Investigation, 2006, p. 20-21, available at: http://www.surreycc.gov.uk/__data/assets/pdf_file/0019/26164/Advice-on-financial-investigation.pdf.

[113] ACPO (Association of Chief Police Officers, UK), Centrex, Practice Advice on Financial Investigation, 2006, p. 21, available at: http://www.surreycc.gov.uk/__data/assets/pdf_file/0019/26164/Advice-on-financial-investigation.pdf.

[114] ACPO (Association of Chief Police Officers, UK), Centrex, Practice Advice on Financial Investigation, 2006, p. 22, available at: http://www.surreycc.gov.uk/__data/assets/pdf_file/0019/26164/Advice-on-financial-investigation.pdf.

[115] ACPO (Association of Chief Police Officers, UK), Centrex, Practice Advice on Financial Investigation, 2006, p. 26-27, available at: http://www.surreycc.gov.uk/__data/assets/pdf_file/0019/26164/Advice-on-financial-investigation.pdf.

[116] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 42.

[117] StAR Initiative, *The Puppet Masters. How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do about It*, 2011, p. 69, available at: http://StAR.worldbank.org/StAR/sites/StAR/files/puppetmastersv1.pdf.

[118] StAR Initiative, *The Puppet Masters. How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do about It*, 2011, p. 71.

[119] StAR Initiative, *The Puppet Masters. How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do about It*, 2011, pp. 72-73.

[120] StAR Initiative, *The Puppet Masters. How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do about It*, 2011, p. 77.

[121] FATF 40 Recommendations against Money Laundering, Recommendation 9.

[122] StAR Initiative, *The Puppet Masters. How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do about It*, 2011,p. 6.

[123] StAR Initiative, *The Puppet Masters. How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do about It*, 2011, pp. 7-8.

[124] StAR Initiative, *The Puppet Masters. How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do about It*, 2011, pp. 35-36.

[125] SHARMAN, J., "Shell companies and asset recovery: Piercing the Corporate Veil", in *Emerging Trends in Asset Recovery*, p.69.

[126] StAR Initiative, *The Puppet Masters. How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do about It*, 2011, Appendix E.

[127] StAR Initiative, *The Puppet Masters. How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do about It*, 2011, pp. 154-155.

[128] StAR Initiative, *The Puppet Masters. How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do about It*, 2011, p. 157.

[129] ATKINSON P., "Asset tracing", in *Emerging trends in Asset Recovery*, p. 228.

[130] ATKINSON P., "Asset tracing", in *Emerging trends in Asset Recovery*, p. 229.

[131] ATKINSON P., "Asset tracing", in *Emerging trends in Asset Recovery*, p. 228.

[132] USAID Nepal, Anticorruption Investigation and Trial Guide: Tools and Techniques to Investigate and Try the Corruption Case, August 2005, p. 29-32, available at: http://pdf.usaid.gov/pdf_docs/PNADE146.pdf.

[133] USAID Nepal, Anticorruption Investigation and Trial Guide: Tools and Techniques to Investigate and Try the Corruption Case, August 2005, p. 34, available at: http://pdf.usaid.gov/pdf_docs/PNADE146.pdf.

[134] Australia, Brunei Darussalam, Canada, Chile, People's Republic of China, Indonesia, Republic of Korea, Malaysia, Mexico, Papua New Guinea, Peru, The Philippines, Russia, Singapore, Thailand, The United States and Viet Nam.

[135] ADB/OECD Anti-Corruption Initiative for Asia and the Pacific, *Mutual Legal Assistance, Extradition and Recovery of proceeds of Corruption in Asia and The* Pacific, 2007, p. 82.

[136] ADB/OECD Anti-Corruption Initiative for Asia and the Pacific, *Mutual Legal Assistance, Extradition and Recovery of proceeds of Corruption in Asia and The* Pacific, 2007, p. 82.

[137] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 127, Box 7.3.

[138] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 127, Box 7.3.

[139] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 75.

[140] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, pp. 75-76.

[141] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 85.

[142] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 75.

[143] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 87-88.

[144] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 77.

[145] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 88.

[146] ADB/OECD Anti-Corruption Initiative for Asia and the Pacific, *Mutual Legal Assistance, Extradition and Recovery of proceeds of Corruption in Asia and The* Pacific, 2007, p. 84.

[147] United Nations Office on Drugs and Crime (UNODC), *Manual on International Cooperation for the purposes of Confiscation of Proceeds of Crime*, 2012, p. 66.

[148] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 75

[149] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 135-136.

[150] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 135-136.

[151] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 76

[152] Thailand Anti-Money Laundering Act, 1999, Section 48.

[153] United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders (UNAFEI), *Effective Measures to Deprive Criminals and Criminal Organizations of Crime Proceeds*, 146th International Training Course, Reports of the Course, p. 95.

[154] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 135-136.

[155] United Nations Convention against Corruption (UNCAC), 2003, articles 31.1.a and 31.1.b.

[156] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 77.

[157] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 79

[158] ADB/OECD Anti-Corruption Initiative for Asia and the Pacific, *Mutual Legal Assistance, Extradition and Recovery of proceeds of Corruption in Asia and The* Pacific, 2007, p. 83.

[159] UNODC, *Manual on International Cooperation for the purposes of Confiscation of Proceeds of Crime*, 2012, par. 193.

[160] UNODC, *Manual on International Cooperation for the purposes of Confiscation of Proceeds of Crime*, 2012, par. 188.

[161] UNODC, *Manual on International Cooperation for the purposes of Confiscation of Proceeds of Crime*, 2012, par. 190.

[162] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 76.

[163] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 79.

[164] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 80.

[165] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 111.

[166] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 80.

[167] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 80-81.

[168] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 108.

[169] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 111.

[170] United Nations Convention against Corruption (UNCAC), 2003, art. 2.

[171] ADB/OECD Anti-Corruption Initiative for Asia and the Pacific, *Mutual Legal Assistance, Extradition and Recovery of proceeds of Corruption in Asia and The* Pacific, 2007, p. 81.

[172] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 79.

[173] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 79.

[174] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 150-151.

[175] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 151.

[176] ADB/OECD Anti-Corruption Initiative for Asia and the Pacific, *Mutual Legal Assistance, Extradition and Recovery of proceeds of Corruption in Asia and The* Pacific, 2007, p. 83.

[177] ADB/OECD Anti-Corruption Initiative for Asia and the Pacific, *Mutual Legal Assistance, Extradition and Recovery of proceeds of Corruption in Asia and The* Pacific, 2007, p. 148-149 and 278.

[178] *Mutual Assistance in Criminal Matters Act 1987* (Cth), section 34J; Proceeds of Crime Act 2002 (Cth), section 19.

[179] ADB/OECD Anti-Corruption Initiative for Asia and the Pacific, *Mutual Legal Assistance, Extradition and Recovery of proceeds of Corruption in Asia and The* Pacific, 2007, p. 165.

[180] ADB/OECD Anti-Corruption Initiative for Asia and the Pacific, *Mutual Legal Assistance, Extradition and Recovery of proceeds of Corruption in Asia and The* Pacific, 2007, p. 175 and 251.

[181] ADB/OECD Anti-Corruption Initiative for Asia and the Pacific, *Mutual Legal Assistance, Extradition and Recovery of proceeds of Corruption in Asia and The* Pacific, 2007, p. 310.

[182] ADB/OECD Anti-Corruption Initiative for Asia and the Pacific, *Mutual Legal Assistance, Extradition and Recovery of proceeds of Corruption in Asia and The* Pacific, 2007, p. 83.

[183] ADB/OECD Anti-Corruption Initiative for Asia and the Pacific, *Mutual Legal Assistance, Extradition and Recovery of proceeds of Corruption in Asia and The* Pacific, 2007, p. 165, 175, 215 and 278.

[184] ADB/OECD Anti-Corruption Initiative for Asia and the Pacific, *Mutual Legal Assistance, Extradition and Recovery of proceeds of Corruption in Asia and The* Pacific, 2007, p. 101 and 251.

[185] ADB/OECD Anti-Corruption Initiative for Asia and the Pacific, *Mutual Legal Assistance, Extradition and Recovery of proceeds of Corruption in Asia and The* Pacific, 2007, p. 83.

[186] Australian *Mutual Assistance in Criminal Matters Act 1987* (Cth), section 34F, Papua New Guinea *Mutual Assistance in Criminal Matter Act 2005*, section 43

[187] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 151-152.

[188] UNODC, *Manual on International Cooperation for the purposes of Confiscation of Proceeds of Crime*, 2012, p. 60.

[189] United Nations Convention against Corruption (UNCAC), 2003, art. 31.3.

[190] UNODC, *Manual on International Cooperation for the purposes of Confiscation of Proceeds of Crime*, 2012, p. 61.

[191] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 81-82.

[192] Basel Institute on Governance, International Centre for Asset Recovery, *Development Assistance, Asset Recovery and Money Laundering: Making the Connection*, 2011, p. 18.

[193] STAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 81-82.

[194] Getting the Deal Through, *Asset Recovery 2015*, Law Business Research, p. 70.

[195] Philippines, Administrative Matter (AM) No. 05-11-04-SC 2015-11-15 (Rule of Procedure in Cases of Civil Forfeiture, Asset Preservation, and Freezing Monetary Instrument, Property or Proceeds Relating to an Unlawful Activity or Money Laundering Offense), Section 21.

[196] Getting the Deal Through, *Asset Recovery 2015*, Law Business Research, p. 19.

[197] Public Works ad Government Services Canada, Seized Property Management Directorate, 2012, available at: http://www.tpsgc-pwgsc.gc.ca/app-acq/gbs-spm/index-eng.html.

[198] United States Marshals Service, Asset Forfeiture Fact Sheet, 2015, available at: http://www.usmarshals.gov/duties/factsheets/asset_forfeiture.pdf.

[199] New Zealand Insolvency and Trustee Service, Criminal proceeds management, 2013, available at: http://www.insolvency.govt.nz/cms/site-tools/about-us/proceeds-of-crime.

[200] In China “the institutions through which the property is seized or detained will manage the property”. Getting The Deal Through, *Asset Recovery 2015*, Law Business Research, p. 44.

[201] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 91-92.

[202] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 101.

[203] New Zealand Insolvency and Trustee Service, Criminal proceeds management, 2013, available at: http://www.insolvency.govt.nz/cms/site-tools/about-us/proceeds-of-crime.

[204] United States Department of Justice, Participants and Roles, 2013, available at: http://www.justice.gov/jmd/afp/05participants/index.htm.

[205] United States Marshals Service, Asset Forfeiture Fact Sheet, 2015, available at: http://www.usmarshals.gov/duties/factsheets/asset_forfeiture.pdf.

[206] United States Department of Justice, Participants and Roles, 2013, available at: http://www.justice.gov/jmd/afp/05participants/index.htm.

[207] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 93.

[208] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 93.

[209] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 94.

[210] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 94.

[211] STAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 95.

[212] UNODC, *Manual on International Cooperation for the purposes of Confiscation of Proceeds of Crime*, 2012, p. 61.

[213] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 95.

[214] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 95-96.

[215] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 95-96.

[216] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 96-97.

[217] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 96-97.

[218] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 97-98.

[219] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 97-98.

[220] UNODC, *Manual on International Cooperation for the purposes of Confiscation of Proceeds of Crime*, 2012, p. 60.

[221] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 98.

[222] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 98.

[223] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 98-99.

[224] Getting The Deal Through, *Asset Recovery 2015*, Law Business Research, p. 87.

[225] Philippines, AM No. 05-11-04-SC 2015-11-15, Section 19.

[226] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 99.

[227] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 99.

[228] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 99.

[229] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 99-100.

[230] StAR Initiative, *Stolen Asset Recovery: A Good Practices Guide for Non-Conviction Based Asset Forfeiture*, 2009, p. 90, available at: https://StAR.worldbank.org/StAR/sites/StAR/files/Non%20Conviction%20Based%20Asset%20Forfeiture.pdf.

[231] Getting the Deal Through, *Asset Recovery 2015*, Law Business Research, p. 19.

[232] StAR Initiative, *Stolen Asset Recovery: A Good Practices Guide for Non-Conviction Based Asset Forfeiture*, 2009, Box 31, p. 91-92.

[233] StAR Initiative, *Stolen Asset Recovery: A Good Practices Guide for Non-Conviction Based Asset Forfeiture*, 2009, p. 92-93.

[234] StAR Initiative, *Stolen Asset Recovery: A Good Practices Guide for Non-Conviction Based Asset Forfeiture*, 2009, p. 93-94.

[235] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 100.

[236] UNODC, *Manual on International Cooperation for the purposes of Confiscation of Proceeds of Crime*, 2012, pp. 65-66.

[237] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 100.

[238] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 100-101.

[239] Getting the Deal Through, *Asset Recovery 2015*, Law Business Research, p. 44, 87 and 160.

[240] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 101.

[241] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 101-102.

[242] United Nations Convention against Corruption (UNCAC), 2003, art. 2

[243] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p.103.

[244] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p.108.

[245] STAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 111.

[246] United Nations Convention against Corruption (UNCAC), 2003, art. 2.

[247] ADB/OECD Anti-Corruption Initiative for Asia and the Pacific, *Mutual Legal Assistance, Extradition and Recovery of proceeds of Corruption in Asia and The* Pacific, 2007, p. 81.

[248] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p.108.

[249] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 108.

[250] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 116-117.

[251] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 117.

[252] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p.7.

[253] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p.111.

[254] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p.112.

[255] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p.113.

[256] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p.111.

[257] Brunei Criminal Asset Recovery Order, 2012, Section 60(1); ADB/OECD Anti-Corruption Initiative for Asia and the Pacific, *Mutual Legal Assistance, Extradition and Recovery of proceeds of Corruption in Asia and The* Pacific, 2007, p. 148, 214 and 278.

[258] United Nations Convention against Corruption (UNCAC), 2003, art. 31; FATF Recommendation 4, available at: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

[259] Anti-Money Laundering Act, 1999, sec. 51 and 52.

[260] STAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p.115-116.

[261] The Confiscation Act, 1987 (Victoria, Australia) and the Proceeds of Crime Act, 2002 (Commonwealth of Australia).

[262] Getting the Deal Through, *Asset Recovery 2015*, Law Business Research Ltd, 2014, p. 32.

[263] Nine Key Principles of Effective Asset Recovery Adopted by the G20 Anticorruption Working Group, Cannes, 2011, available at: http://StAR.worldbank.org/StAR/sites/StAR/files/asset_recovery_country_profiles.pdf.

[264] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 106.

[265] StAR Initiative, *Stolen Asset Recovery. A Good Practices Guide for Non-Conviction Based Asset Forfeiture*, 2009, p. 13.

[266] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 106.

[267] See: the Federal Code of Civil Procedure, available at: http://www.diputados.gob.mx/LeyesBiblio/pdf/6.pdf.

[268] See: Republic of Trinidad and Tobago, Trinidad and Tobago (B.W.I.A. International) Airways Corporation, Trinidad-Tesoro Petroleum Company Limited, and Trinidad and Tobago Racing Authority v. John Frederick Cameron, Litigation Administrator for the Estate of John H. O'Halloran, *et al*, Court file No. 29841/88, Ontario Court of Justice (General Division) Judgment of June 3, 1991, at StAR Asset Recovery Watch cases database, "John H. O'Halloran," at http://StAR.worldbank.org/corruption-cases/node/18517.

[269] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 169.

[270] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 159.

[271] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 159.

[272] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 160.

[273] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 159.

[274] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 106.

[275] Basel Institute on Governance, International Centre for Asset Recovery, *Development Assistance, Asset Recovery and Money Laundering: Making the Connection*, p. 15, available at: https://www.baselgovernance.org/sites/collective.localhost/files/publications/dfid_brochure_final_version_for_print.pdf.

[276] Peru, Law No. 29.212, "Ley que Modifica el Decreto Legislativo N° 922, Decreto Legislativo que Regula el Proceso de Pérdida de Dominio", available at: http://www.cicad.oas.org/fortalecimiento_institucional/legislations/PDF/PE/ley_29212.pdf; Decree No. 1104, "Decreto Legislativo que Modifica la Legislación sobre Pérdida de Dominio", available at: http://www.sbs.gob.pe/repositorioaps/0/2/jer/nac1_segunnormasnacdecretos/2012/DL_1104_%202012.pdf.

[277] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 12.

[278] United Nations Convention against Corruption (UNCAC), 2003, art. 54(1)(c).

[279] Nine Key Principles of Effective Asset Recovery Adopted by the G20 Anticorruption Working Group, Cannes, 2011, available at: http://StAR.worldbank.org/StAR/sites/StAR/files/asset_recovery_country_profiles.pdf.

[280] Nine Key Principles of Effective Asset Recovery Adopted by the G20 Anticorruption Working Group, Cannes, 2011, available at: http://StAR.worldbank.org/StAR/sites/StAR/files/asset_recovery_country_profiles.pdf.

[281] Getting the Deal Through, *Asset Recovery 2015*, Law Business Research Ltd, 2014, p. 19.

[282] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 14.

[283] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 14.

[284] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 107.

[285] StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 107.

[286] United Nations Convention against Corruption (UNCAC), 2003, art. 54-55. StAR Initiative, *Asset Recovery Handbook. A Guide for Practitioners*, 2011, p. 7.

[287] ADB/OECD Anti-Corruption Initiative for Asia and the Pacific, *Asset Recovery and Mutual Legal Assistance in Asia and the Pacific,* Proceedings of the 6th Regional Seminar on Making

International Anti-Corruption Standards Operational, Bali, Indonesia, 5-7 September 2007, p. 66.

[288] ADB/OECD Anti-Corruption Initiative for Asia and the Pacific, *Asset Recovery and Mutual Legal Assistance in Asia and the Pacific,* Proceedings of the 6th Regional Seminar on Making International Anti-Corruption Standards Operational, Bali, Indonesia, 5-7 September 2007, p. 152-153, 155.

[289] See: http://www.dfat.gov.au/issues/measures-against-corruption.html.

[290] Alternative Fines Act available in: http://www.justice.gov/criminal/fraud/fcpa/docs/response2-appx-m.pdf.

[291] Securities Exchange Act of 1934, available at: https://www.sec.gov/about/laws/sea34.pdf. The Act gives the SEC the authority to enter an order "requiring accounting and disgorgement".

[292] KALB, S. and BOHN, M.A., "Disgorgement: The Devil You Don't Know", *Corporate Compliance Insights*, available at: http://www.corporatecomplianceinsights.com/disgorgement-fcpa-how-applied-calculated/.

[293] Securities and Exchange Commission, Plaintiff, Appellee/cross-appellant, v. Robert D. Happ, Defendant, Appellant/cross-appellee, 392 F.3d 12 (1st Cir. 2004), available at: http://law.justia.com/cases/federal/appellate-courts/F3/392/12/598112/

[294] United Nations Convention against Corruption (UNCAC), 2003, art. 57.1.

[295] United Nations Convention against Corruption (UNCAC), 2003, art. 51.

[296] United Nations Convention against Corruption (UNCAC), 2003, art. 57.2.

[297] CLAMAN, D., "The promise and limitations of asset recovery under the UNCAC", in *Recovering Stolen Assets,* 2008, p. 350.

[298] CLAMAN, D., "The promise and limitations of asset recovery under the UNCAC", in *Recovering Stolen Assets,* 2008, p. 329.

[299] In this sense has ruled the Federal Supreme Court of Switzerland in the Marcos case, regarding its own legislation (article 74a § 3 IMAC): that the language used in the law, i.e. 'as a general rule' must be understood as the expression of the willingness of Swiss parliament to leave certain discretion to the Swiss authorities dealing with the execution of Letter Rogatory.

[300] PIETH, M., 'Recovering stolen assets – a new issue', in *Recovering Stolen Assets,* 2008, p. 12 and 13.

[301] GULLY-HART, P., 'International asset recovery of corruption-related assets: Switzerland', in *Recovering stolen assets,* 2008, p. 174.

[302] United Nations Convention against Corruption (UNCAC), 2003, art. 57.3.

[303] United Nations Convention against Corruption (UNCAC), 2003, art. 57.

[304] ADB/OECD Anti-Corruption Initiative for Asia and the Pacific, *Mutual Legal Assistance, Extradition and Recovery of proceeds of Corruption in Asia and The* Pacific, 2007, p. 86.

[305] ADB/OECD Anti-Corruption Initiative for Asia and the Pacific, *Mutual Legal Assistance, Extradition and Recovery of proceeds of Corruption in Asia and The* Pacific, 2007, p. 87.

[306] ATTISSO, K. and FENNER ZINKERNAGEL, G., "Past experience with agreements for the disposal of confiscated assets", in *Emerging trends in Asset Recovery*, 2013, p. 329.

[307] ADB/OECD Anti-Corruption Initiative for Asia and the Pacific, *Mutual Legal Assistance, Extradition and Recovery of proceeds of Corruption in Asia and The* Pacific, 2007, p. 88.

[308] VEGLIO, P., and SIEGENTHALER, P., 'Monitoring the restitution of looted state assets: the role of Multilateral Development Banks (MDBs)', in *Recovering Stolen Assets,* 2008, p. 320.

APEC Project: M SCE 01 12A-1

Produced by

Guillermo Jorge
Governance Latam
La Pampa 1534, 3° A
C1428DZF, Buenos Aires – Argentina

For
Asia Pacific Economic Cooperation
Secretariat 35 Heng Mui Keng Terrace
Singapore 119616
Tel: (65) 68919 600
Fax: (65) 68919 690
Email: info@apec.org
Website: www.apec.org
APEC#215-ES-01.9