Chapter 5

CONDUCTING AND RESPONDING TO INVESTIGATIONS

INTRODUCTION

This chapter will discuss conducting and responding to law enforcement investigations, and when and how financial institutions should conduct their own internal investigations.

LAW ENFORCEMENT INVESTIGATIONS

Law enforcement investigations, in the United States and in many other jurisdictions, can be triggered by any number of factors, including the receipt of what is commonly known as a suspicious transaction report or STR, tips from other sources (inside and outside of the government) and information gleaned from other cases. Once such an investigation is commenced, the relevant law enforcement agency might request information from a financial institution in order to obtain evidence. Requests for information can come in several forms, including subpoenas and search warrants.

Subpoenas are usually issued by grand juries, operating under the purview of a court and empowering a law enforcement agency to compel the production of documents and testimony.
The documents and testimony are designed to allow the law enforcement agency to investigate suspicious transactions, develop evidence and, ultimately, put together a case for prosecution.

A search warrant is a grant of permission from a court for a law enforcement agency to search certain designated premises and to seize specific categories of items or documents. Generally, the requesting agency is required to establish that probable cause exists to believe that evidence of a crime will be located. The warrant is authorized based on information contained in an affidavit submitted by a law enforcement officer.

It should be noted here that, in the United States and several other jurisdictions, the banking regulatory agencies do not need to use subpoenas or search warrants. Their authority to conduct examinations includes the ability to inspect all books and records of a regulated institution.

Steps that law enforcement agencies can or should take in conducting a money laundering investigation include:

- Follow the money. If the agency is aware of where the laundered money originated and/or where it ended up, it is appropriate for the agency to attempt to bring the two ends together and to compile a complete understanding of the flow of the funds.

- Identify the unlawful activity. Most countries define money laundering in terms of predicate offenses or “specified unlawful activities.” These usually are very extensive and include many felony crimes. So for a money laundering case, prosecutors need to establish the flow of money as well as the existence of a predicate offense.

- Document the underlying activity and transactions. This involves documenting not only the underlying predicate offense, but also the flow of funds through various banks and accounts.
Review databases. Financial Intelligence Unit’s (FIU) databases and commercial databases can provide very useful and extensive financial information. Also, records such as “Social Security” information in the United States (i.e., tax related information) can be useful for investigators.

Review public records. Court records, as well as corporate filings and credit reports, can provide useful background information. Also, phone records, real estate Multiple Listing Services (MLS) and newspapers can prove useful.

Review licensing and registration files. Files, such as records held by motor vehicle departments and other registration databases, can provide background information and useful leads.

Analyze the financial transactions and account activity of the target. Look for the normal and expected transactions of the individual or entity based on self-disclosures, income and typical flows of funds by similarly situated persons. If the transactions are outside of the norm or professed anticipated level of activity, then analyze where the additional funds come from and the composition of the unusual activity.

Review STRs that might involve any potential individual linked to the target or the transactions or activity.

Conduct computer-based searches, discussed below.

In cross-border cases, seek international assistance, discussed below.

**Decision to Prosecute**

When considering whether - or to what extent - to bring a case against an institution involving money laundering-related charges, prosecutors typically will look at many factors, including whether:
The institution has a criminal history.

The institution has cooperated with the investigation.

The institution discovered and self-reported the money laundering-related issues.

The institution has had a comprehensive and effective AML program.

The institution has taken timely and effective remedial action.

There are civil remedies available that can serve as punishment.

Deterring wrongdoing by others is needed and will be served by a prosecution.

In the end, however, assuming the case is not simple (“cut and dry”) or egregious, the decision to prosecute will frequently be determined by what the prosecutors believe was the intent of the institution when it undertook the action in question.

**RESPONDING TO A LAW ENFORCEMENT INVESTIGATION**

The first rule when confronted with a law enforcement investigation is to respond quickly and completely to all requests. Failure to do so will only get the institution into more difficulty. If a request is overly broad or unduly intrusive, the institution can attempt to narrow the request or can even seek to contest the request, or portions of the request, in court. However, under no circumstances should an institution ignore, defer or otherwise put aside or delay responding to a law enforcement inquiry or request for documents.

When confronted with a law enforcement inquiry, the financial institution needs to ensure that the appropriate senior management is informed and that someone is designated as being responsible for responding to all law enforcement requests, for monitoring the
progress of the investigation and for keeping senior management informed of the nature and progress of the investigation. If the inquiry appears to be focused on the institution and not just an account or customer, then the Board of Directors should be kept apprised as well. Of course, reports or information about an investigation should not be provided to any employees, officers or directors of the institution who might be implicated in the investigation.

Upon notification of a law enforcement investigation, especially one directed at the institution, consideration should be given to the retention of qualified, experienced legal counsel. Such counsel can guide the institution through the inquiry, contest requests that are perceived to be improper and, ultimately, assist in negotiating settlements if necessary. If the law enforcement inquiry is merely focused on a particular account or is only seeking to obtain financial evidence about a customer and there is no apparent wrongdoing by the institution, there is a less pressing need to obtain counsel. Each case, however, requires individualized review and analysis. This issue is discussed at greater length below.

As set forth below, whenever an institution receives a subpoena, search warrant, or similar law enforcement demand or becomes aware of a government-related investigation involving the institution or one of its accounts or customers, the institution should conduct an inquiry of its own to determine the underlying facts, the institution’s exposure and what steps, if any, the institution should take.

**Summonses and Subpoenas**

If an institution is served with a summons or subpoena compelling the production of certain documents, the institution should have its senior management and/or counsel review the summons or subpoena. If there are no grounds for contesting the summons or subpoena, the institution should take all appropriate measures to comply with the summons or subpoena on a timely and complete basis. Failure to do so can result in adverse action and penalties for the institution.

Also, the financial institution should not notify the customer who is being investigated. If the government asks the bank to keep certain
accounts open, such a request should be obtained in writing under proper letterhead and authority from the government.

**SEARCH WARRANTS**

In some instances, a financial institution may receive a warrant from law enforcement authorities to search its premises.

When a search warrant is served, it is important that everyone present remain calm. Every employee should know that, generally, a search warrant is not an open-ended demand. Instead, it gives the agents the right to enter the premises and to look for and seize certain items or documents. A search warrant does not compel testimony.

When presented with a search warrant, an institution should consider taking the following steps:

- Call the financial institution’s in-house or outside counsel.
- Review the warrant to understand its scope.
- Ask for and obtain a copy of the warrant.
- Ask for a copy of the affidavit that supports the search warrant. The agents are not obligated to provide a copy of the affidavit, but, if a financial institution is allowed to see the affidavit, the financial institution can learn more about the purpose of the investigation.
- Remain present while the agents record an inventory of all items they seize and remove from the premises. Keep track of the records taken by the agents.
- Ask for a copy of law enforcement’s inventory of what they have seized.
- Write down the names and agency affiliations of the agents who conduct the search.
Documents and computer records that are protected by the attorney-client or other legal privilege should be so marked and retained separately from general records. Privileged records should be stored in an area (e.g., cabinet) marked “Attorney-Client Privilege.”

If the agents want to seize these records, institution representatives may object and suggest, as an alternative, that the records be given to the court for safekeeping. All employees should be trained on how to behave in a search, and someone should be designated to communicate with the agents.

**ORDERS TO RESTRAIN OR FREEZE ACCOUNTS OR ASSETS**

If the law enforcement agency or a prosecutor obtains a court order to freeze an account or to prevent funds from being withdrawn or moved, the institution should obtain a copy of the order and should comply with it. Generally, the order is obtained based on a sworn affidavit, which is sometimes included with the order. If the affidavit is not part of the order, the financial institution can ask to see the affidavit, which should provide clues about why a customer’s information is being requested. Whether law enforcement authorities are obligated to provide the affidavit depends on each country’s laws and regulations.

**MONITORING THE INSTITUTION’S RESPONSE TO A LAW ENFORCEMENT INVESTIGATION**

When an institution receives a subpoena, summons or other government request, the institution should do more than just produce the records or information being sought. Financial institutions should ensure that all grand jury subpoenas, as well as other information requests from government agencies, are reviewed by senior management, an investigations group or counsel to determine how best to respond to the inquiry and to determine if the inquiry or the underlying activity might pose a risk to the institution. In addition, the institution should maintain a centralized control over all requests and responses in order
to ensure that the requests are responded to on a complete and timely basis and to establish a complete record of what is provided. This centralized record will also assist with regard to the institution’s own internal investigation.

**DEALING WITH INVESTIGATORS AND PROSECUTORS**

Typically, the most effective strategy is to cooperate with investigators and prosecutors. Providing investigators with the information they need to reach an investigative conclusion may be the most effective way to terminate the investigation before it has a devastating effect on the resources and reputation of the institution. Cooperation may include making employees, including corporate officers, available for interviews, and producing documents without the requirement of a subpoena. It can also include a voluntary disclosure by providing investigators with any report written by counsel regarding the subject under investigation.

The institution should make every effort to stay on good terms with the investigators and prosecutors. At a minimum, a good working relationship will help the institution conduct an effective parallel internal investigation and thereby position the institution to respond more effectively to investigative or prosecutorial inquiries.

It is also important for the institution to try to learn how the investigators and prosecutors view the facts. If they happen to be wrong about some of the facts, the institution will have an opportunity to rectify the situation. At a minimum, if the institution is aware of the investigators’ and prosecutors’ concerns, it will be in a better position to respond to them.

**OBTAINING COUNSEL FOR THE INVESTIGATION**

With regard to particularly large, important or serious investigations, it may be appropriate for the institution to retain counsel to assist in responding to the investigation or advising the institution during the course of the investigation. Many financial institutions, such as large banks and securities dealers, have legal counsel on their staff. But many other financial institutions, such
Conducting and Responding to Investigations

as small money services businesses, do not ordinarily have legal counsel on their payroll. In either case, it is recommended that institutions hire or consult experienced outside legal counsel if confronted with a government investigation of the institution itself.

Using in-house counsel will, of course, cost less, and in-house counsel will start out with a better knowledge of the institution, its personnel, its policies and procedures. However, if the conduct under investigation could involve or lead to a criminal investigation or indictment, outside counsel may be more appropriate.

If the institution determines that it is necessary or appropriate to involve counsel with regard to an investigation, it should take appropriate measures to ensure that the counsel, in-house or outside, is sufficiently experienced and knowledgeable with regard to the factual and legal issues involved. In addition, the institution should determine the nature and scope of the role of counsel and should ensure that senior management is aware of and supports the involvement of counsel.

If the institution is actually facing imminent criminal prosecution or indictment, it needs an experienced criminal litigator. If, however, the investigation appears only to be preliminary or is focused on a single account or customer without necessarily adversely affecting the institution, then obtaining counsel may not be essential.

NOTICES TO EMPLOYEES

With regard to investigations conducted by the government, employees should be informed of the investigation and should be instructed not to produce corporate documents directly, but, rather, should inform senior management or counsel of all requests for documentation and should provide the documents to them for production. In that way, the institution will know what is being requested and what has been produced. In addition, the institution can determine what, if any, requests should be contested. The same procedure should be followed with regard to requests for employee interviews.
MEDIA RELATIONS

People often mistakenly overlook the importance of public and media relations in defending an organization or officer. Public perception is vital to the organization’s success in maintaining public trust.

If the facts are not on the institution’s side, “no comment” may be the best response it can offer. Misleading or false statements such as — “We have no problems and have done nothing wrong.” — can worsen the situation. When such statements are made by a publicly traded company, they can invite additional scrutiny by the SEC and law enforcement agencies.

INTERNAL INVESTIGATIONS

The need for an internal investigation may become apparent as the result of different things, including the following:

- A report of examination from the regulators.
- Information from third parties, such as customers.
- Information derived from surveillance or monitoring systems.
- Information from employees or a company hotline.
- Receipt of a governmental subpoena or search warrant.
- Learning that government investigators are asking questions of institution employees, business associates, customers or even competitors.
- The filing of a civil lawsuit against the institution or a customer of the institution.

The threshold for conducting an internal investigation should be relatively low. Whenever there is unusual or potentially suspicious
activity, an institution should examine the circumstances. The institution may want to develop parameters and thresholds for such internal investigations and may want to sketch out the nature and scope of such investigations, but the institution should always be alert to need to conduct an investigation, especially when one of the above-listed factors is present.

The need to learn the nature and extent of the problem, and the desire to remedy it, and to avoid reputational risk, as well as the need to avoid violating regulatory requirements, all weigh heavily in favor of conducting an internal investigation. The purpose of the investigation will be to learn the nature and extent of any potential wrongdoing, to develop information sufficient to report - when necessary - to the authorities, to enable the institution to minimize its liability, and to stop any potential money laundering.

An internal investigation may help the institution to prepare and respond to any civil, administrative or criminal proceedings. In addition, the fact that an internal investigation was conducted may help mitigate the institution’s exposure to administrative or criminal fines. Further, self-reporting by the institution may also reduce the impact of any administrative or criminal action. As always, the institution should document the purpose of any investigation, the scope of any investigation, how the investigation is conducted, the conclusions reached as a result of the investigation and any follow-up actions taken.

If an investigation is undertaken in response to a government investigation, it is, by definition, reactive in nature, but it should not be otherwise limited. In conducting the investigation, the institution needs to follow the transactions and activity where they lead and needs to make sure at all times that the institution’s AML policies, procedures and controls are sufficient and up-to-date.

If the investigation is generated by internal concerns or reports pertaining to suspicious conduct or potential money laundering, the investigation should similarly be as broad-based as necessary to review not only the underlying activity, transactions and the facts which triggered the investigation, but also to enable the institution to analyze the adequacy of its AML policies, procedures and controls. If any deficiencies are uncovered during the course
of an internal investigation, they should be remedied as soon as possible.

CLOSING THE ACCOUNT

Based on its internal investigation, the institution should make an independent determination as to whether to close the account in issue. Some of the factors that the institution should consider are as follows:

- The legal basis for closing an account.
- The institution’s stated policies and procedures for closing an account.
- How serious is the underlying conduct. If the conduct is serious and rises to the level where the account would ordinarily be closed, then the institution should consider closing the account.
- As stated above, if law enforcement requests the institution to keep the account open, the institution should request that the investigator or prosecutor make that request in writing on proper government agency letterhead with the appropriate authorized signature.

FILING AN STR

In addition, based on its internal investigation, the institution should determine whether or not to file a suspicious transaction report. If the institution decides that it should file an STR, it should notify the investigators or prosecutors as soon as possible.

CONDUCTING THE INVESTIGATION

In the course of conducting an internal investigation, it will nearly always be necessary to: (a) review documents; (b) interview
employees; and (c) generate a written report. Further, it may become necessary to deal with law enforcement investigators and prosecutors. In addition, a determination should be made as to whether and to what extent to involve counsel. Also, procedures should be established to keep senior management - and, when necessary, the board of directors - apprised of the scope and progress of the internal investigation.

DOCUMENTS

THE IMPORTANCE OF GATHERING AND PRODUCING DOCUMENTS

A financial investigator’s main objective is to track the movement of money, whether through a bank, broker-dealer, money services business or casino.

Financial institutions have a wealth of information at their fingertips because they are in the business of taking in, paying out, accounting for and recording the movement of money.

For example, banks maintain signature cards, which are collected at the opening of an account, account statements, deposit tickets, checks and withdrawal items and credit and debit memorandums. Banks also keep records on loans, cashier’s checks, certified checks, traveler’s checks and money orders. They exchange currency, cash third-party checks, and conduct wire transfers, as do most money services businesses. Banks also keep safe-deposit boxes and issue credit cards.

Often, banks are required to keep records of customer accounts for five years. While that rule might vary in different countries, it is important for compliance officers at financial institutions to be aware of these legal requirements. Account records and records of other non-account activities can be essential to tracking possible money laundering.

Other financial institutions keep similar records of transactions and the ability to exert control over an account, such as the ability to
trade stocks in a brokerage account. These records are valuable to an investigator.

In any money laundering investigation, the relevant documents should be examined thoroughly, covering the time frame of the suspected activity, as well as for several months before and after it is thought to have occurred.

According to statements by the U.S. Treasury and Internal Revenue Service (IRS), here are some patterns financial institutions can look for as they investigate possible money laundering:

- Unusually high monthly balances in comparison to known sources of income.
- Unusually large deposits, deposits in round numbers or deposits in repeated amounts that are not attributable to legitimate sources of income.
- Multiple deposits made under reportable thresholds.
- The timing of deposits. This is particularly important when dates of illegal payments are known.
- Checks written for unusually large amounts (in relation to the suspect’s known practices).
- A lack of account activity. This might indicate transactions in currency or the existence of other unknown bank accounts.

(For a more complete list of red flags, see also the chapter on AML programs.)

Frequently, it is a review of documents that turns up information that helps to uncover wrongdoing. Vital information can be found in a wide variety of document types, including internal memos, transactional documents, calendars, e-mails, financial records, travel records, phone logs, signature cards, deposit tickets, checks, withdrawal items, credit and debit memoranda, loan records, etc.

The institution must ensure that relevant documents are not altered, lost or destroyed and that all employees are advised of this
fact. This can be done by a memo sent to all relevant employees. However, if there is concern that such a memo might prompt a particular employee to alter or destroy documents, that situation must be dealt with separately.

The institution should also address its document destruction policy to ensure that no documents are destroyed pursuant to that policy during the investigation. It would not be a serious concern if documents relevant to a government investigation were destroyed, pursuant to a legitimate policy, prior to obtaining knowledge of the investigation or receiving a subpoena. It could, however, be a serious concern if such documents were destroyed, for whatever reason (even pursuant to a legitimate policy), once the institution had been notified about an investigation, even if no subpoena had yet been received.

FINDING AND REVIEWING THE DOCUMENTS

An institution should start by identifying an employee with knowledge of the institution’s files, who will be in charge of retrieving documents for the institution. A system must be put in place to ensure that all documents are located, whether they be in central files, department files, and even individual files. In addition, copies of the same document in different hands should be retrieved. This is important because some copies may have handwritten notes written by the employees who received them.

ORGANIZATION OF DOCUMENTS

The institution should ensure the integrity of original documents, while at the same time minimizing disruption to the institution’s business. It must ensure that an appropriate system is put in place to organize, maintain, number, secure and copy the documents, and to prepare them for production to the government (or to the opposing party in a civil litigation). The documents should be listed in an index, so that they can be found when needed.

A “detailed privilege” log should be created as the documents are gathered, and privileged documents should be kept separate from other documents to help avoid inadvertent disclosure.
INTERVIEWING EMPLOYEES

In addition to securing and reviewing all relevant documentation, it is important to interview all knowledgeable employees. It is important to interview these employees as soon as practicable so that their memories are the freshest and so that they can direct management or counsel to relevant documents and people on a timely basis.

In addition, the institution - usually counsel - should prepare employees who expect to be interviewed by law enforcement investigators and should debrief them after their interviews. The former will help the employee to understand how to handle the process and the latter will assist the institution in better understanding the scope and direction of the government investigation. As stated above, all requests for employee interviews by law enforcement investigators should go through a single person or centralized location.

Most employees are not accustomed or comfortable with being interviewed - either by law enforcement investigators or counsel for the institution. Therefore, care should be given to try and put them at ease to the extent possible.

It is also helpful to have interviews as non-contentious as possible. Background and open-ended questions should be used at the beginning of the interview, together with a non-confrontational review of documents. More contentious questions, if necessary, should be held off for later.

ATTORNEY - CLIENT ISSUES

ATTORNEY-CLIENT PRIVILEGE, APPLIED TO ENTITIES AND INDIVIDUALS

In an internal investigation, all parties should be aware that attorneys for the organization represent the entity and not its employees. Counsel should understand these issues and should conduct the internal investigation accordingly.
There may be major consequences if the interests of an entity and its employees diverge or conflict, or if an employee might implicate the employer or vice versa. In such cases, separate counsel may be required.

DISSEMINATION OF A WRITTEN REPORT BY COUNSEL

If counsel for the institution prepares a written report of an investigation, the institution should take steps to not inadvertently waive the attorney-client privilege by distributing the report to persons who should not receive it. Every page of the report should contain a statement that it is confidential and is subject to the attorney-client privilege and work-product privilege.

Copies of the report should be numbered, and a list of persons who are given copies to read should be maintained. After a set period of time, all copies should be returned. Persons obtaining the report should be instructed not to make notes on their copies. All copies should be maintained in a file separate from regular institution files in a further effort to maintain the highest level of protection.

EXPLOITING THE INTERNET FOR MONEY LAUNDERING INVESTIGATIONS

The investigator should start with a metasearch1 — using a number of different search engines — and then move to specific search engines with different capabilities. From the metasearch, the investigator can also start narrowing the parameters using keywords. That enables the investigator to focus on opportunities, identifying an individual’s habits, education, interests and use of the Internet.2

1 A metasearch engine is a search tool that sends user requests to several other search engines and/or databases and aggregates the results into a single list or displays them according to their source.

2 The following section is based on material from John Pyrik, CAMS, a Canadian AML expert with a broad range of analytical and investigative experience.
To know your customer and perform due diligence, you will need information from internal and external sources. Right now, on your computer, you have access through the Internet to perhaps 10 billion pages of external information. This is an amazing resource, but to exploit it, you need two things: thinking skills and technical skills.

**Too Much Money**

Take, for example, the case of a gas station owner who deposits $50,000 in cash per week. Is this money laundering? Many people would simply plug the owner’s name into Google (or other search engine) and consider that search sufficient. A better approach would be to ask: How much cash do gas stations of that size and location typically deposit? This leads to a very different line of inquiry. If you are lucky, your internal sources may provide an answer, but, if not, perhaps the Internet could lead you to news stories, marketing studies, or businesses for sale which might provide useful clues about the cash flow of comparable gas stations.

The Internet might also reveal useful information about the area where the gas station is located: population statistics, income levels, ethnicity, crime rates, etc. Is it located on a commuting corridor? Are there competitors nearby? Does it have a car wash or a convenience store attached?

By comparing the suspect business with others and examining the context, it becomes possible to argue that there is “…a high level of cash deposits atypical of the expected business profile” — a classic indicator of money laundering.

**Unknown Business**

Often, the thinking skills of a savvy Internet investigator involve creatively combining information from different websites. This was how an unknown business was identified.

The case involved a bank client who was depositing large amounts of cash in his personal account. The bank suspected that its client
was operating an unlicensed money remittance service out of the back of his restaurant. They were about to file a suspicious transaction report when they realized that they were missing a key piece of information: the name of the client’s restaurant. How did they solve the mystery? They began by assuming that the client’s restaurant was near the bank. Using a simple online telephone directory they were able to generate a list of all the restaurants within one mile of the bank.

But which one belonged to the client? They needed a way to look up incorporation records for each of the businesses that they had identified. Not wanting to use a commercial service like LexisNexis, they went to a free online public records provider. Clicking on the jurisdiction, then the link for corporations, led them to the right government department, where they inputted the name of each one of the area restaurants until they found one with their client listed as a director.

What is the moral of the story? It is a common mistake to think that the Internet will jump you straight to the information you need. Often, as in the case above, there are several steps and lots of dead ends. Success usually depends on taking what you learn from one site and using it to refine your search on
another. This particular case had an interesting twist at the end. A Google or other search engine search for the restaurant found an advertisement in an online business directory. The advertisement contained a “dead link” to the website for the restaurant. Undaunted, the investigator realized two things:

- Someone registered the site.
- A copy might still exist somewhere.

It was a simple matter to look up the domain name registration.

Finding an old version of the website required a visit to an internet archive provider, where inputting the website address uncovered over a dozen copies, each one a snapshot preserving what the website looked like at a specific moment in time.

For someone conducting due diligence on a business, it could be quite useful to look back in time using one of these sites to see how the business evolved. How did the business change? Who were their former suppliers and clients? Where was it located? Who has left the company?

**WEIRD WIRES**

What technical skills are useful for Know Your Customer (KYC) and due diligence? Let’s say, for example, that you had to research a woman named Cynthia Jenkins in Albuquerque, New Mexico, who has received 13 wire transfers, each for $9,900, in the last two weeks. Your first step might be to confirm that Cynthia actually exists, using “high value” sites.

- Is she listed in the telephone directory? Try a website that collects results from all the leading search engines.
- Is she mentioned in any public records? Try a public records search engine.

Could this be a case of identity theft? Imposters often use the Social Security Numbers of dead people. Fortunately, in the United States, it is possible to check the Social Security Death Index by
searching for “Social Security Death Index” using your favorite search engine.

Your second step might be to search the web for any mention of Cynthia.

But, do you use a directory or a search engine? How do you structure your searches? What keywords do you use?

There are good tutorials on the web for those who want to improve their search skills. There are also sites that tell you about search engines and others for professional searchers. The easiest and most effective way to improve your web-searching skills is to read the “Help” pages of major search engines and to try out their advanced features.

Some tips on search engines:

- Using multiple search engines is a good idea, since no single engine covers the entire web.
- If you are searching in a foreign country, use a local search engine.
Use metasearch engines.

A third step might be accessing a commercial database.

While these databases require the payment of a fee, public record aggregators can be worth the fee, as they cross-reference a huge number of records.

**The Final Word**

It’s one thing to have technical competency; it’s another to be able to sift through all the information you can find online and come up with something meaningful.

Hopefully, these three scenarios demonstrate that there is more to using the web than simply being a proficient searcher. To be successful, you must also bring to the keyboard your area knowledge and your thinking skills.

**AML Cooperation Between Countries**

Practices that restrict international cooperation between supervisory authorities or Financial Intelligence Units in analyzing and investigating suspicious transactions or money laundering crimes, confiscating assets or extraditing accused money launderers are serious obstacles to combating money laundering.

Here are some methods for international AML cooperation.

**International Money Laundering Information Network** — The International Money Laundering Information Network (IMoLIN) serves as a clearinghouse of money laundering information for the benefit of national and international anti-money laundering agencies. It was developed and is administered by the Global Program against Money Laundering of the United Nations Office on Drugs and Crimes (UNODC) on behalf of the UN and other
international organizations, including Interpol. IMoLIN has five main features, all but one accessible to the public:

- **AMLDID:** Anti-Money Laundering International Database - A compendium and analysis of national AML laws and regulations, as well as information on national contact and authorities. The database is password-protected.

- **Reference Data:** Research and analysis, bibliography, conventions, legal instruments and model laws.

- **Country Page:** Includes full text of AML legislation where available, and links to national FIUs.

- **Calendar of Events:** Chronological listing of training events, conferences, seminars, workshops and other meetings in the AML field.

- **Current Events:** Current news of recent AML initiatives.

**Mutual Legal Assistance Treaties**

The classic gateway, usually embodied in a treaty for mutual legal assistance (MLAT), provides a legal basis for transmitting evidence that can be used for prosecution and judicial proceedings.

If evidence is required from another jurisdiction, a request can be made for mutual legal assistance. Procedures vary, but, generally, the following happens:

- The central authority of the requesting country sends a “commission rogatoire” (letters rogatory, or letter of request) to the central authority of the other country. The letter includes the information sought, the nature of the request, the criminal charges in the requesting country and the legal provision under which the request is made.

- The central authority that receives the request sends it to a local financial investigator to find out if the information is available.
An investigator from the requesting country then visits the country where the information is sought, and accompanies the local investigator during visits or when statements are taken.

The investigator asks the central authority for permission to remove the evidence to the requesting country.

The central authority sends the evidence to the requesting central authority, thereby satisfying the request for mutual legal assistance.

Local witnesses may need to attend court hearings in the requesting country.

FINANCIAL INTELLIGENCE UNITS

The second official gateway involves a communication between Financial Intelligence Units (FIUs) or other bodies set up to fight money laundering and other financial crimes.

Generally, FIUs are agencies that receive reports of suspicious transactions from financial institutions and other persons and entities, analyze them, and disseminate the resulting intelligence to local law-enforcement agencies and foreign FIUs to combat money laundering.

The first few FIUs were established in the early 1990s in response to the need for a central agency to receive, analyze and disseminate financial information to combat money laundering. Over the following years, the number of FIUs increased to the point where the Egmont Group, the informal international association of FIUs, now has more than 100 members.

In 2003, the Financial Action Task Force (FATF) adopted a revised set of recommendations on combating money laundering that, for the first time, included explicit recommendations for the establishment and functioning of FIUs.
Although the FIU members of the Egmont Group share the same core functions of receiving, analyzing, and disseminating financial information to combat money laundering and financing of terrorism, they often differ in how they are established and how they function.

A 2004 Report “Financial Intelligence Units: An Overview” by the International Monetary Fund said that although, in establishing an FIU, authorities may feel the need to respond to the calls of the international community, their decisions as to the FIU’s functions and the modalities of its operations need to be based on the country’s own crime-fighting policy objectives, resources and priorities. The responsibilities of the FIU also need to be harmonized with those of existing national agencies involved in the fight against financial crime, including law enforcement, supervisory agencies and policy-setting government bodies. Moreover, the establishment of an FIU will entail the use of budgetary resources.

When establishing an FIU, the IMF said that the following needs to be kept in mind:

- Objectives to be pursued by the establishment of the FIU need to be defined.
- The FIU must be given the means to successfully pursue these objectives, for which it will become accountable.
- Care should be taken not to give the FIU more responsibilities than it can handle, given its expected resources. In some cases, other agencies that have resources and experience may be in a position to exercise certain functions, such as the supervision of AML/CFT requirements, in a more effective way than an FIU.
- Overlapping functions should be avoided to the extent possible, and, to the extent such overlap is unavoidable, coordination mechanisms should be established to minimize conflicts and to maximize cooperation between the concerned agencies.
In many countries, it has been found productive to discuss the proposed FIU and the draft law with the representatives of the segments of the private sector that will be most directly affected by the establishment of the new AML/CFT regime. Early consultations with the private sector will also provide an opportunity for the government authorities to explain the benefits of the new system to firms that will have to begin reporting transactions to the FIU.

The FIUs, with the task of receiving and analyzing suspicious transaction reports and maintaining close links with police and customs authorities, share information among themselves informally in the context of investigations, usually on the basis of memoranda of understanding (MOU). The Egmont Group of FIUs has established a model for such MOUs. Unlike the MLAT, this gateway is not ordinarily used for obtaining evidence, but for obtaining intelligence that might lead to evidence.

The FIUs participating in the Egmont Group want to encourage cooperation among and between themselves in the interest of combating money laundering and terrorist financing. The members issued a document on “Principles of Information Exchange Between Financial Intelligence Units,” adopted in June 2001 and incorporated into the Group’s Statement of Purpose.

Some countries may restrict the exchange of information with other FIUs or the access to information requested by an FIU. This document describes practices that maximize cooperation between FIUs and can be useful to government authorities when considering anti-money laundering legislation.

Furthermore, to address practical issues that impede mutual assistance, the document provides guidelines in terms of best practices for the exchange of information between FIUs. When dealing with international information requests, FIUs are urged to try to take these best practices into account to the greatest possible extent.

Here are some principles included in the document:

- The Egmont principle of free exchange of information at the FIU level should be possible on the basis of reciprocity, including spontaneous exchange.
■ Differences in the definition of offenses that fall under the competence of FIUs should not be an obstacle to free exchange of information at the FIU level. To this end, the FIU’s competence should extend to all predicate offenses for money laundering, as well as terrorist financing.

■ The exchange of information between FIUs should take place as informally and as rapidly as possible and with no excessive formal prerequisites, while guaranteeing protection of privacy and confidentiality of the shared data.

■ Should an FIU still need a Memorandum of Understanding to exchange information, it should be negotiated and signed by the FIU without undue delay. To that end, the FIU should have the authority to sign MOUs independently.

■ It should be possible for communication between FIUs to take place directly, without intermediaries.

■ Providing an FIU’s consent to disseminate the information for law enforcement or judicial purposes should be granted promptly and to the greatest extent possible. The FIU providing the information should not deny permission to disseminate the information unless doing so would fall beyond the scope of its AML/CFT provisions, could impair a criminal investigation, would be clearly disproportionate to the legitimate interests of an individual or legal person or the country of the providing FIU, or would otherwise not be in accord with basic principles of national law. Any refusal to grant consent should be appropriately explained.

The following practices should be observed by the FIU requesting the information:

■ All FIUs should submit requests for information in compliance with the Principles for Information Exchange set out by the Egmont Group. Where
applicable, the provisions of information-sharing arrangements between FIUs should also be observed.

- Requests for information should be submitted as soon as the precise assistance required is identified.

- When an FIU has information that might be useful to another FIU, it should consider supplying it spontaneously as soon as the relevance of sharing this information is identified.

- The exchange of information between Egmont FIUs should take place in a secure way. To this end, the Egmont FIUs should use the Egmont Secure Web (ESW) where appropriate.

**Explanation of FIU sharing process within the EU**

In 2004, the European Commission awarded a grant to the Ministry of Justice in the Netherlands to create the FIU.NET and to take on the development of highly sophisticated electronic connections among European Union Member State Financial Intelligence/Investigations Units. FIU.NET is a decentralized computer network designed to connect FIUs of the EU using modern technology and computers to bilaterally exchange financial intelligence information. FIU.NET encourages co-operation and enables FIUs to exchange intelligence quickly, securely and effectively. This, in turn, further helps encourage sharing of information. The main purpose of this increased cooperation is to further the fight against organized crime and against the misuse of the financial system for the purpose of money laundering and terrorist financing.

The Egmont Group has developed a form for requesting information. The use of this form should be encouraged when exchanging information. Requests should contain sufficient background information to enable the requested FIU to conduct a proper analysis/investigation. Requests should be accompanied
by a brief statement of relevant facts known by the requesting FIU. Unless indicated otherwise, all requests for information originating from another FIU should be answered as soon as possible. FIUs should assign unique case reference numbers to both outgoing and incoming requests to facilitate tracking. In acknowledging a request, the responding FIU should provide the requesting unit with the name and contact details, including telephone and fax numbers, of the contact person and the case or reference number assigned to the case. The FIU should strive to reply within one week if the request involves information it has direct access to or if it is unable to provide an answer due to legal impediments.

Whenever the requested FIU needs to have external databases searched or must query third parties (such as financial institutions), it should reply within one month of getting the request. The FIU may consider contacting the requesting unit within a week of receipt to state that it has no information directly available and that external sources are being consulted or that it is experiencing difficulties answering the request. That response can be made orally. If the results of the inquiries are still not all available after a month, the requested FIU should provide the information it already has in its possession or at least indicate when it will be able to answer completely.

FIUs should consider establishing mechanisms to monitor request-related information, enabling them to detect new information they receive regarding transactions, STRs, etc., that are involved in previously received requests. Such a monitoring system would enable FIUs to inform requestors of new and relevant material related to their earlier requests.

Where the requested FIU wants to know how the information it provided was used, it should request this explicitly. When the requesting FIU is not able to give this feedback, it should reply with the reasons why it cannot be provided. If appropriate, especially in case of urgent requests, and in order to speed up proceedings, prior consent for further use of information can be granted with the reply itself.

All FIUs should use the greatest caution when dealing with supplied information in order to prevent any unauthorized use resulting in a breach of confidentiality.
THE SUPERVISORY CHANNEL

The Basel Committee on Banking Supervision, in its April 2002 “Report on Sharing of Information between Jurisdictions in Connection with the Fight against Terrorism,” cites the supervisory channel as the third official gateway. It says that with regard to banking, information from supervisory agencies is normally of a general character and is designed to monitor the financial soundness of a banking group. Increasingly, however, inquiries relate more to specific assets or accounts because of concerns about reputational and legal risks.

One example concerns accounts for Politically Exposed Persons (PEPs), a term used for public officials in the civil or military arms of government, who can be recipients of funds derived from public corruption. The ability to share information is often defined by the legal framework under which the supervisory agency operates, but it may also be supported by an MOU. Unlike an MLAT, an MOU is not a treaty and usually is not binding on governments. Instead, it reflects an agreement among supervisory authorities. An MOU may be especially valuable with such entities as securities or trading firms, which fall within the jurisdiction of a specific regulatory authority. Information communicated through this gateway usually is provided for supervisory purposes only, and may not ordinarily be used as evidence or shared widely among governmental entities.

The Committee also indicated that enforcement agents should reach out through proper channels to FIUs, central banks and banking superintendents to determine the filing, reporting and licensing requirements applicable to the subjects of their investigations. In this way, they can determine what records they can reach through legal process, where to get the witnesses to introduce them into evidence, document compliance (or lack of) and rebut defenses.
FATF RECOMMENDATIONS ON COOPERATION BETWEEN COUNTRIES

The FATF developed its 40 Recommendations or best practices as a basic framework for establishing and maintaining effective AML programs worldwide. They cover the criminal justice system and law enforcement, the financial system and its regulation, and international cooperation. (For more, see the chapter on International Standards.)

Recommendations 36 – 40 from the FATF’s 40 Recommendations pertain specifically to the international aspects of money laundering and terrorist financing investigations. They deal with mutual legal assistance treaties, extradition, confiscation of assets and mechanisms to exchange information internationally.

SUMMARY

It is important, and in most cases legally mandated, for financial institutions to establish and follow a comprehensive and adequate anti-money laundering (AML) program. In addition, institutions must be aware of the possibility of investigations by law enforcement agencies and how to respond to them. Also, institutions need to be aware of the potential need to conduct their own internal investigations. In connection with this, institutions should be aware of the investigatory and search capabilities of the Internet, which is constantly changing. Last, institutions need to be familiar with the international bases and mechanisms for cross-border sharing.
Review Questions

- What are the basic situations in which an internal investigation might be appropriate?
- When a financial institution is served with a search warrant, what should it do?
- How can you do research on the Internet for money laundering investigations?
- What are gateways for cross-border information sharing in money laundering investigations or cases?