

# CHAPTER 4

## ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM

### INTRODUCTION

**A**n anti-money laundering program is an essential component of a financial institution's compliance regime. The primary goal of every good program is to protect the organization against money laundering and to ensure that the organization is in full compliance with relevant laws and regulations. For that reason, designing, structuring and implementing these programs should be the top priorities of any institution.

An AML program should be risk-based, and should be designed to mitigate the money laundering and terrorist financing risks the organization may encounter. The risk-based nature of the program recognizes that not all aspects of an institution's business present the same level of risk. Certain aspects of the business a financial institution conducts will pose greater money laundering risks than others and will require additional controls to mitigate these risks, while others will present a minimal risk and will not need the same level of attention. More detail will be provided on risk later.

Depending on the size of the organization, the anti-money laundering function may be a stand-alone department or may

be performed by persons who have other compliance duties. Regardless of the size of the organization, there should be some centralized aspect of control that has an organization-wide view of AML efforts within the organization. The AML program should establish minimum standards for the organization that are reasonably designed to comply with applicable laws and regulations. The organization-wide program may be supplemented by the policies and procedures of various lines of business or legal entities that address specific areas, such as private banking, trade finance, cash handling or investigations. Compliance programs should also include corporate governance and overall management of money laundering and terrorist financing risks.

Before designing an anti-money laundering program, it is imperative to understand what is required of an institution, its employees and customers by the laws and regulations of the jurisdiction where the institution is located. The financial institution's internal policies and risks related to the business must also be taken into consideration. Anyone needing advice on the complexities of anti-money laundering legislation before building an anti-money laundering program should consult a competent advisor, even if it means seeking outside help.

In this section, we will discuss what to consider when designing a compliance program; how to assess risk; how to spot, manage, document and follow up on suspicious activities; how to know your customer and employee; how to audit your program effectively; and what you need to know about training and screening employees.

## ASSESSING RISK AND DEVELOPING A RISK-SCORING MODEL

---

### INTRODUCTION

---

Understanding what is legally required of your institution, employees and customers is essential to a successful program.

Whatever those legal requirements, however, FATF, along with numerous member countries, such as the United Kingdom and United States, urge risk-based controls.

The theory is that no financial institution can reasonably be expected to detect all wrongdoing by customers, including money laundering. But if an institution develops systems and procedures to detect, monitor and report the riskier customers and transactions, it will increase its chances of staying out of harm's way from criminals and from government sanctions and penalties.

A risk-based approach requires institutions to have systems and controls that are commensurate with the specific risks of money laundering and terrorist financing facing them. Assessing this risk is, therefore, one of the most important steps in creating a good anti-money laundering compliance program. As money laundering risks increase, stronger controls are necessary. However, all categories of risk — whether low, medium or high — must be identified and mitigated by the application of controls, such as verification of customer identity, CDD policies, suspicious activity monitoring and economic sanctions screening.

Governments around the world believe that the risk-based approach is preferable to a more prescriptive approach in the area of anti-money laundering and counter-terrorist financing because it is more:

- **Flexible** — as money laundering and terrorist financing risks vary across jurisdictions, customers, products and delivery channels, and over time.
- **Effective** — as companies are better equipped than legislators to effectively assess and mitigate the particular money laundering and terrorist financing risks they face.
- **Proportionate** — because a risk-based approach promotes a common sense and intelligent approach to fighting money laundering and terrorist financing as opposed to a “check the box” approach. It also allows

firms to minimize the adverse impact of anti-money laundering procedures on their low-risk customers.

## FACTORS TO DETERMINE RISK

The risks your organization faces depend on many factors, including the geographical regions involved, your customer types and the products and services offered.

Risk is dynamic and needs to be continuously managed. It is critical that risk ratings accurately reflect the risks present, provide meaningful assessments that lead to practical steps to mitigate the risks, are periodically reviewed and, when necessary, are updated. Make sure you evaluate new business products for money laundering vulnerabilities and implement appropriate controls before launching them into the market.

But what exactly is a risk-based approach, and what might a risk-scoring model look like? You can ask the following questions to assess an institution's vulnerabilities to money laundering and terrorist financing:

## WHAT RISKS DO YOUR CUSTOMERS POSE?

---

### LEVELS OF RISK

Generally, all risk categories can be broken down into the following levels of risk:

- **Prohibited** — The company will not tolerate any dealings of any kind given the risk. Countries subject to economic sanctions or designated as state sponsors of terrorism, such as Sudan or Iran, are prime candidates for prohibited transactions. Prohibited customers would include shell banks.
- **High-Risk** – The risks here are significant, but are not necessarily prohibited. To mitigate the heightened risk presented, the firm should apply more stringent

controls to reduce the risk, such as conducting enhanced due diligence and more rigorous transaction monitoring. Countries that are noted for corruption or drug trafficking are generally deemed high risk. High-risk customers may include PEPs; high-risk products and services may include correspondent banking and private banking.

- **Medium-Risk** — Medium risks are more than a low- or standard-risk of money laundering, and merit additional scrutiny, but do not rise to the level of high-risk.
- **Low- or Standard-Risk** — This represents the baseline risk of money laundering; normal business rules apply. FATF member countries and domestic retail customers are frequently, but not always, considered to be standard- or low-risk.

A risk-scoring model generally uses numeric values to determine the category of risk (geography, customer type and products and services), as well as the overall customer risk. For example, each category could be given a score between 1 and 10, with 10 being the riskiest. The individual categories could be scored with 1-3 being standard risk, 4-8 being medium risk and 9-10 being high risk. This is particularly helpful when looking at product risk, as it will help determine appropriate controls for the products.

The three categories are then combined to give a composite score. A simple model would just add the totals from the categories, which would yield a score between 3 and 30. The model can be made more complex by weighting each of the factors differently, such as putting more emphasis on the type of customer, as opposed to the product or country. The model can be made even more sophisticated by, for instance, creating combinations of factors that will determine the overall rating. The degree of complexity is up to the institution; the more complex, the more likely the rating will reflect the customer's overall risk. However, the more complex the model is, the more difficult it may be to determine the risk rating on an on-going basis, particularly as customers add more products and services or, for business customers especially, as they expand into new markets.

It is when the categories are combined that the customer's risk picture becomes clearer. For instance, when you combine a product with a customer type, the combination can radically change the level of risk. If you have a small, foreign, private company seeking to open a checking account with online wire transfer capabilities, you may not have much information on the customer. When such a customer has the ability to rapidly transfer funds, the resulting risk level may be higher. In this case, the customer may have higher risk ratings for geography, customer type and products and services. However, if a domestic company listed on a major stock market wants to establish an employee retirement plan, it must provide a lot of information as part of being listed on the major stock market and may not be very vulnerable to money laundering, so the risk will probably be much lower.

A "high" risk assessment number does not mean that a prospective customer should automatically be denied an account. The number is more useful in determining which individuals or groups might require greater scrutiny.

The next step is to determine, based on the scoring methodology chosen, what thresholds to establish for each risk category. The institution should be mindful that the high-risk relationships should not represent too large a segment of the population; this is not to say the scores should be adapted to fit the customer portfolio, rather, because high-risk customers truly do need more attention, which costs more money, the institution needs to be mindful that it needs to make a profit. In addition, if the portfolio is overly weighted toward high-risk, even if the institution appears to be making a profit, the overall risk level in the institution may be too great to support.

Generally, it is good to periodically reassess the risk-rating criteria to see if the customers that are scored as a higher risk are those that are more likely to create issues. If they aren't, it may be time to reassess the risk-scoring model.

## GEOGRAPHICAL LOCATION

A crucial step in devising any risk-scoring model involves jurisdictional risk. In what countries or jurisdictions do your

individual customers reside and what are the customers' countries of citizenship? Where are your corporate customers headquartered and where do they conduct the majority of their business? Some might be located in countries with a higher risk of money laundering.

There is no definitive, independent system for assessing the money laundering risks of various territories and countries. Some firms will devise their own methods; others will look to a vendor solution. Whichever course is chosen, it is essential that the risk-rating methodology be documented. When looking specifically at money laundering risk, the terrorism and sanctions lists published by governments and international organizations can be a useful starting point. These include lists published by the United Kingdom's Financial Services Authority, U.S. Office of Foreign Assets Control, the U.S. Financial Crimes Enforcement Network, the European Union, the World Bank and the United Nations Security Council Committee. A model should also take into account whether the country is a member of FATF or of a FATF-style regional body and has AML requirements equivalent to international best practices.

Companies might also consider the overall reputation of the countries in question. In some, cash may be a standard medium of exchange. Others may have politically unstable regimes and high levels of public or private sector corruption. Some may have a reputation as a bank secrecy haven. Still others may be widely known to have high levels of internal drug production or to be in drug transit regions. How can one identify such countries? The U.S. State Department issues an annual "International Narcotics Control Strategy Report" rating more than 100 countries on their money laundering controls. Transparency International publishes a yearly "Corruption Perceptions Index," available at [www.transparency.org](http://www.transparency.org), which rates more than 100 countries on perceived corruption. Monitoring major news media is also recommended, and care should be taken that all of the country lists are monitored on a regular basis for changes. Also, the quality of a country's anti-money laundering laws and regulations, and the strength of its financial industry, can be factors in determining risk.

## CUSTOMER TYPE

This factor looks at the various types of clients, such as individuals, listed companies, private companies, joint ventures, partnerships, financial institutions and others who want to establish a relationship with the institution. To whom are you selling your products? Money remittance companies? Foreign public officials? Travel agencies? Other financial institutions?

A vital step in risk assessment is the analysis of the users of the products and services that the institution or business offers. Based on the answers to these questions and others, to what extent is your institution or business at risk of money laundering and terrorist financing? Those who have a history of involvement in criminal activities receive the highest ratings. Political figures or those in political organizations score toward the top of the scale, higher than officials of multinational corporations. For example, when a bank is approached by a private company, the risk is higher than it would be with a corporation listed on a major stock exchange because the due diligence that can be conducted is more limited with the former. If you have a considerable amount of publicly available information, there should be a lower risk than with a small company that is not listed and for which public information is not available.

Risks are generally higher if a money launderer can hide behind corporate veils such as trusts, charities, limited liability companies or structures where it is difficult to identify the beneficial owners of the money. The risk is even higher if corporations are based in countries with inadequate anti-money laundering requirements or strict corporate secrecy protections.

Regulators in various countries have said that the following types of customers might be considered high-risk for money laundering:

- Casinos;
- Offshore corporations and banks located in tax/banking havens;
- Leather goods stores;
- Currency exchange houses, money remitters, check cashers;



- Car, boat and plane dealerships;
- Used-car and truck-dealers and machine parts manufacturers;
- Travel agencies;
- Brokers/dealers in securities;
- Jewel, gem and precious metals dealers;
- Import/ export companies; and
- Cash-intensive businesses (restaurants, retail stores, parking).

While it may not work for all customer types, certain types of customers may merit special treatment when it comes to risk-rating. For instance, not every non-bank financial institution presents the same level of risk. Accordingly, a more nuanced approach might be used to break down the various risk factors, such as the type of non-bank financial institution, the quality of supervision over the business, the strength and adequacy of the business' AML program, the volume of activity the non-bank financial institution does with the institution and the nature of the relationship the customer has had with the institution.

## WHAT RISKS DO YOUR PRODUCTS OR SERVICES POSE?

An important element of risk assessment is to review new and existing products and services that the institution or business offers to determine how they may be used to launder money or finance terrorism. The compliance officer should be an active participant in project teams identifying appropriate control frameworks for new products and systems.

What products and services does your institution offer that may be vulnerable to money laundering or terrorist financing? Internet accounts? Private banking? Money transmittal services? Stock brokerage services? Annuities? Insurance products? Offshore services? Money orders? Correspondent banking? Sale of major non-financial goods and services, such as automobiles and real estate?

This risk-rating, based on the type of product the customer seeks, is calculated using a number of product-related factors. Most notably, it depends on the likelihood that the product requested might be used for money laundering or terrorist financing. You probably won't see interest-rate swaps being used to finance terror, but securities may be another matter. Product scoring is not universal because different financial institutions face varying degrees of risk.

Questions to ask include: Does a particular new or current product or service:

- Enable significant volumes of transactions to occur rapidly?
- Allow the customer to engage in transactions with minimal oversight by the institution?
- Afford significant levels of anonymity to the users?
- Have an especially high transaction or investment value?
- Allow payments to third parties?
- Have unusual complexity?
- Require government verification of customer eligibility?

In addition, certain specific banking functions or products are considered high-risk. These include:

- Private banking;
- Offshore international activity;
- Deposit-taking facilities;
- Wire transfer and cash-management functions;
- Transactions in which the primary beneficiary is undisclosed;
- Loan guarantee schemes;

- Travelers checks;
- Official bank checks;
- Money orders;
- Foreign exchange transactions;
- Trade-financing transactions with unusual pricing features; and
- Payable Through Accounts (PTAs).

## THE ELEMENTS OF AN AML PROGRAM

---

In general, the basic elements a financial institution or business must address in an anti-money laundering program are:

- A system of internal policies, procedures and controls;
- A designated compliance officer with day-to-day oversight over the AML program;
- An ongoing employee training program; and
- An independent audit function to test the AML program.

## INTERNAL POLICIES, PROCEDURES AND CONTROLS

---

The first step in determining what policies, procedures and controls are necessary is to identify and understand the applicable laws and regulations. This will set the absolute minimum compliance standards for the institution. The institution should then look at its own risk assessment and gauge its risk appetite. For example, what countries, products and customers are prohibited because the institution has deemed them to be too risky? These should be prohibited by policy and should be supported by appropriate controls to enforce the policy. Institutions also need a process to stay on top of regulatory changes, which will keep the program current.

Internal anti-money laundering policies should be established or approved by higher management or the board of directors, and should set the tone for the organization. While the organization's policy may be a high-level statement of principles, it serves as the basis for procedures and controls that provides details as to how lines of business will achieve compliance with laws and regulations, as well as with the organization's AML policies.

#### Example

The purpose of our AML policy is to establish the general framework for the fight against money laundering, terrorism, corruption and other financial crimes. Successful participation in this fight by the financial sector requires an unprecedented degree of global cooperation between governments and financial institutions. Our institution is committed to reviewing our AML strategies and objectives on an ongoing basis and to maintaining an effective AML program. We are committed to high standards of AML compliance and require management and employees to adhere to these standards in preventing the use of our products and services for money laundering purposes. Adherence to this policy is absolutely fundamental for ensuring that all of our entities, regardless of geographic location, comply with applicable anti-money laundering legislation. We are required and committed to adhere to minimum standards of anti-money laundering compliance based on the applicable anti-money laundering laws and regulations and any additional standards from our regulatory supervisors which clarify the main statutory duties imposed on our institution. In any country/jurisdiction where the requirements of applicable anti-money laundering laws establish a higher standard, our entities located in those jurisdictions must meet those standards. Our AML program is formulated and directed by the anti-money laundering department, but it is the responsibility of all employees to keep ill-gotten funds out of our institution.

The standard AML operating procedures are often designed and drafted at a lower level in the organization and are modified as needed to reflect changes in products, personnel and promotions, and other day-to-day operating procedures. They are more detailed than the policies. Standard operating procedures translate policy into an acceptable and workable practice. In addition to policies and procedures, there should also be a process to support and facilitate effective implementation of procedures, and that process should be reviewed and updated regularly.

While policies and procedures provide important guidance, the AML program also relies on a variety of internal controls, including management reports and other built-in safeguards that keep the program working. These internal controls should enable the compliance officer to recognize deviations from standard procedures and safety protocols. A matter as simple as requiring an officer's approval or two signatures for transactions that exceed a prescribed amount could be a critical internal control element that, when ignored, seriously weakens an institution's money laundering controls.

Similarly, a "second review" of actions considered to be departures from policy could be helpful if subsequent questions arise. For example, an employee who approves a seemingly innocuous exception from internal policy by allowing the purchase of certain monetary instruments for cash could inhibit detection of a pattern of money laundering activity. A second review could prevent this. Other effective controls use technology, such as account opening systems that force the entry of required information; aggregation systems that detect reportable currency transactions; and automated account monitoring programs.

Policies and procedures should be in writing, and must be approved by appropriate levels of management. In general, institution-level policies should be approved by the board, while business unit procedures can be approved by business unit management.

An AML compliance program should include policies, procedures, and processes that:

- Identify high-risk operations (products, services, customers, and geographic locations); provide for periodic updates to the institution's risk profile; and provide for an AML compliance program tailored to manage risks.
- Inform the board of directors (or a committee of the board) and senior management of compliance initiatives, known compliance deficiencies, suspicious transaction reports filed and corrective action taken.
- Assign clear accountability to persons for performance of duties under the anti-money laundering program.
- Provide for program continuity despite changes in management or employee composition or structure.
- Meet all regulatory requirements and recommendations for anti-money laundering compliance.
- Provide for periodic review as well as timely updates to implement changes in regulations. Generally, this should be done at least on an annual basis.
- Implement risk-based CDD policies, procedures and processes.
- Provide sufficient controls and monitoring systems for the timely detection and reporting of suspicious activity. (Institutions should consider centralizing their own review and report-filing functions.)
- Provide for dual controls and segregation of duties. Employees who complete the reporting forms should not also be responsible for filing the reports or granting the exemptions.
- Comply with all recordkeeping requirements, including retention and retrieval of records.
- Provide sufficient controls and monitoring systems for the timely detection and reporting of activity, such as for large currency or large transaction reporting.

- Provide for adequate supervision of employees who handle currency transactions, complete reports, grant exemptions, monitor for suspicious activity, or engage in any other activity covered by the anti-money laundering laws, including implementing regulations.
- Train employees to be aware of their responsibilities under anti-money laundering laws, regulations and internal policy guidelines.
- Incorporate anti-money laundering compliance into the job descriptions and performance evaluations of appropriate personnel.
- Develop and implement screening programs to ensure high standards when hiring employees. Implement sanctions for employees who consistently fail to perform in accordance with an AML framework.
- Develop and implement program testing to assess the effectiveness of the program's implementation and execution of its requirements. This is separate from the independent audit requirement, but serves a similar purpose — to assess the effectiveness of the program.

How to structure your anti-money laundering department is a critical issue. The solution depends on the size of your institution and staff, as well as the nature and range of the products and services you offer. A clear definition of how the anti-money laundering department should be administered and by whom are vital questions that must be answered at the start.

## COMPLIANCE OFFICER

---

A person should be designated as the anti-money laundering compliance officer. This individual should be responsible for designing and implementing the program, making necessary changes and disseminating information about the program's successes and failures to key staff members, constructing anti-money laundering-related content for staff training programs and staying current on legal and regulatory developments in the field.

The exact structure of a money laundering prevention department varies with each institution. Sometimes, one person is responsible for strategic aspects of the program, and another person is responsible for its operational aspects, including suspected money laundering monitoring and reporting suspicious activity.

The department can be organized into subgroups. Examples include:

- The Investigations Group: Monitors alerts generated on customer transactions, such as those from automated systems, as well as referrals from line of business staff. The group also investigates such alerts and referrals and files Suspicious Transaction Reports (STRs) with the Financial Intelligence Unit (FIU) as required.
- Line of Business Support Group: Assigns a risk code to all clients based on scoring of the CDD risk assessment, performs additional due diligence on medium- and high-risk clients identified via the CDD process and provides a first line of contact for line of business questions on AML matters.
- The Program Oversight Group: Performs periodic reviews and updates of the program, coordinates implementation activities with the line of business support group to ensure that line of business procedures get updated to incorporate program changes, and monitors regulatory environment for changes to the program. Also may be involved in preparing training materials and providing guidance and advice on more complicated AML issues not addressed by the line of business support group. This group generally would have primary responsibility for coordinating regulatory examinations with the lines of business.

Often, in addition to these three groups, other anti-money laundering tasks are conducted in the business lines, wherever there is customer contact. For example, CDD forms are often completed by account officers and others at the point where a



new account is opened, and branch colleagues participate in periodic reviews of high-risk clients and may be required to provide additional information or explanation to support investigations into potentially suspicious activity. Sometimes, suspicious activity may be reported to the Corporate Security group which, upon determining that the activity may pose an AML risk, may refer the case to the Investigations Group. The compliance department may also direct anti-money laundering-related compliance efforts as a result of instructions from a regulatory authority or other research findings.

## TRAINING

Regulations and laws require financial institutions to have formal, written AML compliance programs that include “training for appropriate personnel.” A successful training program not only should meet the standards set out in the laws and regulations that apply to an institution, but should also satisfy internal policies and procedures and should mitigate the risk of getting caught up in a money laundering scandal. Training is one of the most important ways to stress the importance of anti-money laundering efforts, as well as educating employees about what to do if they encounter potential money laundering. In this discussion of training, the term includes not only formal training courses, but it also includes communication that serves to educate and inform employees, such as e-mails, newsletters, periodic team meetings and anything else that facilitates the sharing of information.

Let’s explore some basic elements behind the development of effective compliance training.

## WHO TO TRAIN

The first step in designing an effective training program is to identify the target audience. Most areas of the institution should receive AML training, and the target audience should include most employees. But each segment should be trained on topics and issues that are relevant to them.

Example

- **Customer contact staff:** This is your front line of defense against money laundering; the ones who need the deepest practical understanding of why anti-money laundering efforts are important and what they need to do to be vigilant against money laundering. While a general course will often be able to address the importance of AML and to provide some basics, some additional training on specific unit procedures may be in order, depending on the nature of the course and the institution. For example, loans, credit and loan operations staff need training that reflects an understanding of the credit function and how money launderers might misuse credit products, how the staff might recognize potential money laundering and what they must do if they see it. Cash handlers often need special training, as many jurisdictions have imposed additional requirements to address the increased risk posed by cash. These employees need to know how to properly handle the cash transactions, especially those that trigger reporting requirements.
- **Back office personnel:** These employees may also need special training. Some, like proof operators, may not have a need for specialized training beyond some general training, but others, such as staff in the cash vault, wire transfer operations, and trade finance operations, may well need specialized training.
- **Audit and compliance staff:** These are the people charged with overseeing, monitoring and testing money laundering controls, and they should be trained about changes in regulation, money laundering methods and enforcement, and their impact on the institution.
- **AML Compliance staff:** These are the people who run the AML program. While they likely do not need the general AML course that would be provided to most employees, this group needs specialized training to be able to stay on top of new trends or changes that

impact the institution and the way it manages risk. Often, this will require attending conferences or AML-specific presentations that go into greater detail.

- **Senior management and board of directors:** Money laundering issues and dangers should be regularly and thoroughly communicated to the board. It is important that the compliance department has strong board support, and one way to ensure that is to keep board members aware of the reputational risk that money laundering poses to the institution.

## WHAT TO TRAIN ON

After the target audience is defined, the next factor in designing an effective training program is identifying the topics to be taught. This will vary according to the institution and the specific products or services it offers.

Several basic matters should be factored into AML training:

- General information: background and history pertaining to money laundering controls, what money laundering and terrorist financing are, why the bad guys do it, and why stopping them is important;
- Legal framework: how AML laws apply to institutions and their employees;
- Penalties for anti-money laundering violations, including criminal and civil penalties, fines, jail terms, as well as internal sanctions, such as disciplinary action up to and including termination of employment;
- How to react when faced with a suspicious client or transaction;
- How to respond to customers who want to circumvent reporting requirements;
- Internal policies, such as customer identification and verification procedures and CDD policies;

- What are the legal recordkeeping requirements;
- Suspicious transaction reporting requirements;
- Currency transaction reporting requirements; and
- Duties and accountability of employees.

The person responsible for designing the training must identify which, if any, of these topics relate to the target audience.

Effective training should present real-life money laundering schemes, preferably cases that have occurred at the institution or at similar institutions, including, where applicable, how the pattern of activity was first detected, its impact on the institution and its ultimate resolution.

## HOW TO TRAIN

Here are some steps that trainers can take to develop the “how” of an effective training program:

- Identify the issues that must be communicated and decide how best to do this. Sometimes a memo or e-mail message will accomplish what is needed without formal, in-person training. Sometimes, e-learning can efficiently do the job. Sometimes, classroom training is the best option.
- Identify the audience by functional area as well as by level of employee/management. This should be accompanied by a quick “why are they here” assessment. New hires should receive training different from that given to veteran employees.
- Determine the needs that should be addressed. There may be issues uncovered by audits or exams, or created by changes to systems, products or regulations.
- Determine who can best develop and present the training program.

- Create a course abstract or curriculum that addresses course goals, objectives and desired results. Be sure to identify who the audience should be and how the material will be presented.
- To the extent possible, establish a training calendar that identifies the topics and frequency of each course.
- Consider whether to provide handouts. The purpose of most training handouts is either to reinforce the message of the training or to provide a reference tool after the fact. Keep them simple.
- If tests are used to evaluate how well the message is received, copies of the answer key should be made available. Similarly, if a case study is used to illustrate a point, provide a detailed discussion of the “preferred course of action.”
- Attention span is a factor to consider. Focus on small, easy to digest, easy to categorize issues.
- Track attendance. Ask attendees to sign in, and issue reminders if make-up sessions are needed. Unexcused absences may warrant disciplinary action and notation in employee personnel files.

## WHEN TO TRAIN

The location and time of day for training are also important. Try to minimize trainees’ time away from work. The time immediately after lunch is the “black hole” for compliance training. Factors unique to each institution will shape the schedule for training. For example, some have administrative policies that require training to be conducted during regular hours to minimize the expense of overtime pay. Other institutions allow for training on non-work days or before or after business hours to minimize disruptions. Regular training scheduled at the end of a month or quarter may be inconvenient for certain departments and employees who have routine month- or quarter-end responsibilities. Training sessions

that coincide with critical system conversions or other one-time labor-intensive events probably will not be well attended. While an institution's training should be regular and ongoing, situations may arise that demand an immediate session. For example, an "emergency" training session may be necessary right after an examination or audit that uncovers serious money laundering control deficiencies. Or a newspaper headline that names the institution might prompt quick-response training. Changes in software, systems, procedures or regulations may trigger the need for an unforeseen training session.

## WHERE TO TRAIN

Some institutions have training centers that allow trainees to escape the distractions of daily work activity. Some types of training are more effective when conducted in small groups, such as the evaluation of a money laundering case study. Role-playing exercises, which may be used to complement a prepared lecture or panel discussions, also are more effective in small groups. These training sessions can be held anywhere. Large group training can be done via telephone conference calls, videos, Internet, auditorium teaching and other impersonal methods.

## AUDIT

Putting your AML compliance program into motion is not enough. The program must be monitored and evaluated. Institutions should assess their anti-money laundering programs regularly to ensure their effectiveness and to look for new risk factors.

The audit must be independent (i.e., performed by people not involved with the organization's AML compliance staff), and individuals conducting the audit should report directly to the board of directors or to a designated board committee composed primarily or completely of outside directors. Those performing the audit must be sufficiently qualified to ensure that their findings and conclusions are reliable.

The independent audit should:

- Address the adequacy of AML risk assessment.
- Examine the adequacy of CDD policies, procedures and processes, and whether they comply with internal requirements.
- Determine personnel adherence to the institution's AML policies, procedures and processes.
- Perform appropriate transaction testing, with particular emphasis on high-risk operations (products, services, customers and geographic locations).
- Assess training adequacy, including its comprehensiveness, accuracy of materials, training schedule and attendance tracking.
- Assess compliance with applicable laws and regulations.
- Examine the integrity and accuracy of management information systems used in the AML compliance program.
- Evaluate the system's ability to identify unusual activity by:
  - Reviewing policies, procedures, and processes for suspicious activity monitoring.
  - Evaluating the system's methodology for establishing and analyzing expected activity or filtering criteria.
  - Evaluating the system's ability to generate monitoring reports.
  - Determining whether the system's filtering criteria are reasonable.
- If an automated system is not used to identify or aggregate large transactions, the audit should include a sample test check of tellers' cash proof sheets, tapes

or other documentation to determine whether large currency transactions are accurately identified and reported.

- Review Suspicious Transaction Reporting (STR) systems, which should include an evaluation of the research and referral of unusual transactions. Testing should include a review of policies, procedures and processes for referring unusual or suspicious activity from all business lines (e.g., legal, private banking, foreign correspondent banking) to the personnel or department responsible for evaluating unusual activity.
- Assess the effectiveness of the institution's policy for reviewing accounts that generate multiple suspicious transaction report filings.
- Assess the adequacy of recordkeeping.
- Track previously identified deficiencies and ensure management corrects them.
- Decide whether the audit's overall coverage and frequency are appropriate to the risk profile of the organization.
- Consider whether the board was responsive to earlier audit findings.
- Determine the adequacy of the following, as they relate to the training program and materials:
  - ❑ The importance the board and senior management place on ongoing education, training and compliance.
  - ❑ Employee accountability for ensuring AML compliance.
  - ❑ Comprehensiveness of training, in view of specific risks of individual business lines.
  - ❑ Training of personnel from all applicable areas of the institution.



- ☐ Frequency of training.
- ☐ Coverage of internal policies, procedures, processes and new rules and regulations.
- ☐ Coverage of different forms of money laundering and terrorist financing as they relate to identifying suspicious activity.
- ☐ Sanctions for noncompliance with internal policies and regulatory requirements.

Make sure any self-assessments or external audits are accompanied by a written report to management outlining who conducted the assessment, the methods used to assess the program, the results and any suggested changes. The assessments or audits to identify deficiencies may be performed by employees of the institution or business, but not by persons who administer the program.

After an audit is complete, financial institutions must implement necessary changes. Share the findings with employees who are directly involved in the deficiencies that need to be corrected. Solicit the advice of these employees on how they feel the program could work better. For record-keeping, you may want to set deadlines for each change and list the person who is primarily responsible for getting it done. Keep detailed records of audits and change implementations. Examiners may request them. Failure to properly address audit issues is a frequent criticism in cases where regulators levy fines on institutions.

## COMPLIANCE CULTURE AND SENIOR MANAGEMENT'S ROLE

---

Embedding a compliance culture into the overall institutional culture is key to an effective AML program. Staff in the business lines sometimes feel that they are overwhelmed by other priorities. Sometimes, the culture of immediate, short-term profit takes precedence over the culture of compliance with anti-money

laundering laws and regulations. It is dangerous, though, when compliance staff is ignored, viewed as irrelevant, or is placed too far away from the business units. It is critical that firms establish a strong culture of compliance that guides and reinforces employees as they make decisions and choices each day. Raising awareness, to the point where everyone in the organization feels compelled to deter and detect money laundering, is vital.

Ultimate responsibility for the AML compliance program rests with the board of directors. Members must set the tone from the top by openly voicing their commitment to the program, ensuring that their commitment flows through all service areas and lines of business, and holding responsible parties accountable for compliance.

The board's role in AML compliance consists of reviewing and approving the overall AML program and ensuring that there is on-going oversight. That does not mean that board members are expected to become anti-money laundering experts themselves, or that they are responsible for day-to-day program management. Rather, it means that they should formally approve an institution's AML compliance program and then make sure the program is adequately implemented and maintained by staff.

The board's oversight role also extends to the supervisor's examination process. Examiners routinely converse with the board and management before and during an on-site exam; they wish to gauge the board's commitment to compliance, its understanding of the law, and its knowledge of how the institution operates. A poor response by the board during these discussions will be a significant red flag and will likely lead to a more thorough examination.

Once an exam by a supervisor or auditor is conducted, it is the board's duty to ensure that any necessary corrective action is taken. Specific duties can be delegated, but the board will be responsible if problems cited by the examiner or auditor are not corrected.

In light of the fact that the cooperation of senior managers is crucial, as you develop your compliance program you must make sure they are kept informed of your progress and approve of each step along the way. Keep necessary parties informed and solicit

their suggestions. Anti-money laundering compliance is not just one person's job. Every manager and staff member is responsible in his or her own way for helping to prevent money laundering abuses. Disseminating that message from senior managers is vital to a successful program.

An adequate AML program costs money, which management may be reluctant to spend. The AML officer's challenge is to convince management that, while an AML program may cost money, it is an indispensable expense to protect the institution and to avert legal problems and reputational harm for the institution. One only needs to look at the fines and penalties levied by regulators to see the costs of non-compliance. However, the cost of the fine is only part of the overall expense; significant additional costs include legal bills, potential loss of business due to reputational damage, extensive compliance review charges, consulting fees, costs for system and other compliance program enhancements, as well as the opportunity costs as the compliance staff and others will be spending the bulk of their time addressing the consent order. It is far better to be able to build the system your institution needs at a more relaxed pace than within the timeframes dictated by a formal consent order.

Senior management must show its commitment to compliance by:

- Establishing a strong compliance plan that is approved by the board of directors and is fully implemented.
- Insisting that it be kept informed of compliance efforts, audit reports and any compliance failures, with corrective measures instituted.
- Communicating compliance expectations to the institution personnel.
- Including regulatory compliance within the job descriptions and job performance evaluations of institution personnel.
- Implementing procedures, processes and controls to ensure compliance with the AML program.

- Conditioning employment on regulatory compliance.

Anti-money laundering units generally are considered cost centers required to protect financial institutions from regulatory risks. A compliance officer who is trying to obtain approval by the board of directors and senior management of the anti-money laundering program can point out that the information collected during the CDD process can be used to sell additional products. The key to maximizing the AML unit's usefulness is to share valuable data with other areas of the firm, not just with law enforcement agencies, regulators and senior management. As AML units build their CDD files, they can identify information other departments can use to sell products and to expand profits. For example, marketing departments that better understand the activity of certain retail or business customers can more effectively cross-sell products and analyze the overall customer relationship.

Before releasing customer information, it is important to review applicable privacy laws and the firm's privacy policy to understand any limitations. Generally, there are no regulatory problems with sharing customer information with other internal departments. However, some firms restrict the sharing of customer information outside the organization or allow customers to "opt-out" of the right for the firm to provide their information to third-party companies.

Compliance staff should generally also be sufficiently independent of the line of business they support so that potential conflicts of interest are minimized. The compliance staff should not be provided an incentive based on the profitability of the line of business they support. While this does not mean the compliance staff shouldn't get bonuses, it means that incentives should not be structured in a way that might create a conflict of interest. While the compliance staff may sit within the line of business and report to line management, it should have the ability to escalate issues without fear of recrimination to a compliance or risk management function outside the line of business. This is not to say that the compliance staff should not be close to the line of business; on the contrary, a close working relationship with the line of business is crucial to successful execution of the AML program. Ultimately, the compliance staff should be seen as a trusted advisor by the line,

so that the line will come to the compliance staff when they have questions and will follow the advice provided.

## CUSTOMER DUE DILIGENCE

Many experts say that a sound Customer Due Diligence (CDD) program is the best way to prevent money laundering. Knowledge is what the entire anti-money laundering compliance program is built upon. The more you and your institution know, the better money laundering abuses can be prevented.

### MAIN ELEMENTS OF A CDD PROGRAM

A sound CDD program should include these 7 elements:

- Full identification of customer and business entities, including source of funds and wealth when appropriate.
- Development of transaction and activity profiles of each customer's anticipated activity.
- Definition and acceptance of the customer in the context of specific products and services.
- Assessment and grading of risks that the customer or the account present.
- Account and transaction monitoring based on the risks presented.
- Investigation and examination of unusual customer or account activity.
- Documentation of findings.

## ACCOUNT OPENING, CUSTOMER IDENTIFICATION AND VERIFICATION

---

A sound CDD program should have reliable customer identification and account opening procedures. Institutions should adopt account opening procedures that allow them to determine the true identity of customers. Institutions should set identification standards tailored to the risk posed by particular customers. In some countries, authorities have issued specific regulations and laws that set out what institutions are required to do regarding customer identification.

What follows includes account opening and customer identification guidelines from the February 2003 General Guide to Account Opening and Customer Identification, an Attachment to the Basel Committee publication Customer Due Diligence for Banks, a guide to good practices related to customer identification.

This document, which was developed by the Working Group on Cross-Border Banking, does not cover every eventuality, but, instead, focuses on some of the mechanisms banks can use in developing effective customer identification programs.

Each new customer who opens a personal account should be asked for:

- Legal name and any other names used (such as maiden name).
- Correct permanent address (the full address should be obtained; a postal box number is usually not sufficient).
- Telephone and fax numbers and e-mail address.
- Date and place of birth.
- Nationality.
- Occupation, position held and name of employer.
- An official personal identification number or other unique identifier contained in an unexpired, official, government-issued document (e.g., passport,

identification card, residence permit, driver's license) that bears a photograph of the customer.

- Type of account and nature of the banking relationship.
- Signature.

The institution should verify this information by at least one of the following methods:

- Confirming the date of birth from an official document (e.g., birth certificate, passport, identity card).
- Confirming the permanent address using an official document (e.g., utility bill, tax assessment, bank statement, letter from a public authority).
- Contacting the customer by telephone, letter or e-mail to verify the information supplied after an account has been opened (a disconnected phone, returned mail, or incorrect e-mail address should warrant further investigation).
- Confirming the validity of the official documentation either by physical verification of the original or through certification by an authorized person (e.g., embassy official).

These examples are not the only possibilities. In some jurisdictions, other documents of an equivalent nature may be offered as satisfactory evidence of a customer's identity.

When appropriate, institutions should also obtain information about the source of wealth, source of funds and the customer's line of business, and should investigate the source of funds of large deposits, especially when they are made in cash or are disproportionate to the customer's declared source of income. Officials should consider the proximity of the customer's residence or place of business to the branch where the account is opened, and, if it is not close by, determine why the customer is opening an account at that location.

Financial institutions should apply equally effective customer identification procedures for non-face-to-face customers as for those available for interview.

For corporate entities (e.g., corporations and partnerships), the following information should be obtained:

- Name of institution.
- Principal place of its business operations.
- Mailing address.
- Names of primary contact people or those authorized to use the account.
- Contact people's telephone and fax numbers.
- Some form of official identification number, if available (e.g., tax identification number).
- The original or certified copy of the Certificate of Incorporation, Memorandum and Articles of Association.
- The resolution of the Board of Directors to open an account and identification of those who have authority to operate the account, including beneficial owners.
- Nature and purpose of business, and its legitimacy.

The institution should verify this information by at least one of the following methods:

- For established corporate entities, review a copy of the latest report and accounts (audited, if available).
- Conduct an inquiry by a business information service, or obtain an undertaking from a reputable firm of lawyers or accountants (or, in some countries, verifying officers) confirming the documents submitted.



- Undertake a company search or other commercial inquiries to see that the institution has not been, or is not in the process of being, dissolved or terminated.
- Use an independent information verification process, such as by accessing public and private databases.
- Obtain prior bank references.
- Visit the corporate entity, where practical.
- Contact the corporate entity by telephone, mail or e-mail.

The institution should also take reasonable steps to verify the identity and reputation of any agent who opens an account on behalf of a corporate customer, if that agent is not an officer of the customer. For more details, please see the reference materials.

The exact account opening procedures and customer acceptance policies depend on the type of customer, the risk and the local regulations.

Once the customer is identified and the account is opened, the institution should monitor the account as part of its CDD process. The frequency of monitoring depends on the risk of the customer. The institution should categorize the customers (see section on “Risk Assessment”) depending on the risk they present and should monitor accordingly. Some categories of customer will not require frequent monitoring because their activities are routine and unexceptional, while other customers that pose a heightened risk of money laundering will require greater due diligence and monitoring. Institutions should implement ongoing monitoring systems to identify suspicious activity, including transactions that are not compatible with the profile or stated business purpose of that particular customer.

In conducting your CDD, in certain circumstances, you may want to identify the major clients and suppliers of your high-risk customers, especially those with large and frequent transactions.

#### Real Life Case

The New York branch of Jordan-based Arab Bank was assessed a \$24 million civil money penalty in August 2005 for inadequate money laundering and terrorist financing controls in its funds transfer and clearing operations. The penalty, issued jointly by the U.S. Financial Crimes Enforcement Network (FinCEN) and Office of the Comptroller of the Currency (OCC), followed two other enforcement actions against the branch — the bank's sole presence in the United States — in February 2005 by the OCC. The earlier actions required the branch to preserve asset levels, pay off depositors and improve its compliance program and internal controls. They also required the branch to convert to an uninsured agency office with limited banking activities and to shut down its wire transfer operations. Arab Bank New York acted mainly as an intermediary institution, clearing funds transfers for members of the Arab Bank Group in other countries and for domestic and foreign correspondent banks outside the Arab Bank Group. But the bank monitored the transactions of its direct customers only, FinCEN said. Following the penalty assessment, Arab Bank stated that it "did not believe the law required [the same money laundering controls it had applied to its direct customers] to be applied to wire transfers in which the branch had only an intermediary role." But the customer base and geographic locations of the Arab Bank Group and correspondent institutions, and the volume of funds transfers of the branch, posed heightened risks of money laundering and terrorist financing, FinCEN said. The branch did not have mechanisms to identify, investigate and report potentially suspicious activity related to funds transfers by non-accountholders appropriate for its risk, which resulted in the non- and late filing of suspicious transaction reports. FinCEN also criticized the branch for not using publicly available information and Office of Foreign Assets Control lists to monitor transactions.

A written Customer Identification Program (CIP) must be included within the institution's AML compliance program and must include, at a minimum, policies, procedures and processes for the following:

- Identifying information required to be obtained (including name, address, taxpayer identification number and, for individuals, date of birth), and risk-based identity verification procedures (including procedures that address situations in which verification is not possible).
- Complying with recordkeeping requirements.
- Checking new accounts against prescribed government lists, if applicable.
- Providing adequate notice about customer identification requirements.
- Covering the institution's reliance on other financial institutions or third parties, if applicable.
- Determining whether and when suspicious transaction reports should be filed.
- Conducting a risk analysis of customers for account opening purposes, which consider the types of accounts offered, methods of account opening, and the institution's size, location and customer base.
- Opening new accounts for existing customers.
- Obtaining the approval of the board of directors, either separately for the CIP or as part of the AML compliance program.
- Conducting audit and training programs to ensure that the CIP is adequately incorporated.
- Verifying that all new accounts are checked on a timely basis against prescribed government lists for suspected terrorists or terrorist organizations.

## NAME CHECKING LISTS

Before a financial institution starts doing business for the first time with a new customer, it should check published lists of known or suspected terrorists for a potential match.

One of the best-known lists is the U.S. Treasury's Office of Foreign Assets Control's Specially Designated Nationals and Blocked Persons list. Updated often, it contains hundreds of names of individuals and businesses the U.S. government considers to be terrorists or international narcotics traffickers and others that are covered by U.S. foreign policy and trade sanctions. Many other sanctions are based on United Nations and other international mandates.

In the United States, compliance with OFAC rules must be a top priority. Although OFAC is not a financial institution supervisory agency, it works closely with them at federal and state levels. Bank examiners routinely ask to see the OFAC compliance manual during examinations, and they conduct tests for OFAC compliance.

U.S. financial institutions are alert to transactions that involve OFAC-designated names. When they spot such a transaction, they are obligated not only to block or reject it, but also to notify OFAC.

Be advised, however, that even thorough due diligence procedures and OFAC searches do not always detect suspicious high-risk individuals and businesses your organization needs to avoid.

Financial institutions and businesses that receive lists of suspected terrorists from government agencies have learned that screening customer lists for suspected terrorists from Middle Eastern countries is not easy. Most of the names of "designated terrorists" on the OFAC lists numerous "Also Known As" alternative names.

An understanding of Arab naming customs and protocols could alleviate the confusion. While some multiple names may be aliases, others are confusing because the customs are not understood.

- All names are transliterated from an Arabic script in which short vowels are most often left out. So the

name Mohammed might be written on a financial account as Mohamed or Mohamad.

- Arabic names are typically long. A person's second name is the father's name. If a "bin" or "ibn" precedes the name, it indicates "son of." If a family name is included at the end, it will sometimes have "al" preceding it.
- There is widespread use of certain names such as "Mohamed," "Ahmed," "Ali," or any name with the prefix "Abd-" or "Abdul," which means "servant of," and is followed by one of 99 suffixes used to describe God.
- Many Arabic names begin with the word "Abu." If it is a first name, it is probably not the person's given name, because "Abu" means "father of." "Abu," followed by a noun, means something like "freedom" or "struggle," and is used by both terrorists and legitimate political leaders. Only when "Abu" is a prefix of a surname should it be accepted as a given name.

Even with all the precautions your compliance program may take to know your customer, the best program can fail. For example, there still is no clear way to designate and identify Politically Exposed Persons (PEPs). Accepting corruption proceeds from PEPs may be money laundering under some countries' laws as it is in the United States. The Financial Action Task Force makes explicit reference to PEPs in its 40 Recommendations.

But a practical issue remains in the view of many AML professionals: How can this high-risk category of customer and the possible corrupt source of his or her money be identified? The problem is the lack of available and useful information about the identity of PEPs around the world. Currently, there are dozens of private providers, that offer a PEPs database, however, the information contained in them and the ability to positively match your customer with a PEP on a database can be a challenge. In addition, as additional scrutiny has been placed on PEPs, they have gotten more creative in finding ways to avoid detection, such as opening accounts in the names of corporations instead of in

their own names or the names of close family members. (On the other hand, looking at geographical issues, the size and nature of an account, and the purpose of the account may by themselves raise PEP-related issues.)

The “Corruption Perceptions Index” published by Transparency International, an international non-governmental organization devoted to combating corruption, could be useful in focusing on high-risk jurisdictions. However, not every customer from a country in the top 10 list of perceived corrupt countries is a PEP. Moreover, even a PEP from a low-risk jurisdiction may not be above bribery, extortion and other corruption.

Some government agencies, such as the U.S. Central Intelligence Agency, already publish lists of Heads of State and Cabinet Members of Foreign Governments. Lists are on its website at [www.cia.gov](http://www.cia.gov). But this list does not provide all relevant information because, for instance, there is no unique identifier, such as a date of birth or address. This results in significant operational constraints, particularly at large retail financial institutions.

## CONSOLIDATED CDD

According to the Basel Committee, a global risk management program for CDD should incorporate consistent identification and monitoring of customer accounts globally across business lines and geographical locations, as well as oversight at the parent level, in order to capture instances and patterns of unusual transactions that might otherwise go undetected.

Such comprehensive treatment of customer information can significantly contribute to a bank’s overall reputational, concentration, operational and legal risk management through the detection of potentially harmful activities, says the Committee.

Firms should aim to apply their customer acceptance policy, procedures for customer identification, process for monitoring higher risk accounts and risk management framework on a global basis to all of their branches and subsidiaries. The firm should

clearly communicate these policies and procedures to ensure that they are fully adhered to.

Each office of the group should be in a position to comply with minimum identification and accessibility standards applied by the head office. However, some differences in information collection and retention may be necessary across jurisdictions to conform to local requirements or relative risk factors.

Where the minimum CDD standards of the home and host countries differ, offices in host jurisdictions should apply the higher standard of the two. Where this appears not to be possible, the institution should confer with its home office and attorneys.

## KNOW YOUR EMPLOYEE

Institutions and businesses have learned at great expense that an insider can pose the same money laundering threat as a customer. It has become clear in the AML field that having equal programs to know your customer and to know your employee are essential.

A Know Your Employee (KYE) program means that the institution has a program in place that allows it to understand an employee's background, conflicts of interest and susceptibility to money laundering complicity. Policies, procedures, internal controls, job descriptions, code of conduct/ethics, levels of authority, compliance with personnel laws and regulations, accountability, monitoring, dual control, and other deterrents should be firmly in place.

Background screening of prospective and current employees, especially for criminal history, is essential to keeping out unwanted employees and identifying those to be removed.

The Federal Deposit Insurance Corporation (FDIC), a U.S. regulator, has provided guidance on employee screening in its paper "Pre-Employment Background Screening: Guidance on Developing an Effective Pre-Employment Background Screening Process," issued in June 2005.

Background screening can be an effective risk-management tool, providing management with some assurance that the information provided by the applicant is true and that the potential employee has no criminal record. Used effectively, the pre-employment background checks may reduce turnover by verifying that the potential employee has the requisite skills, certification, license or degree for the position; may deter theft and embezzlement; and may prevent litigation over hiring practices. An institution should verify that contractors are subject to screening procedures similar to its own.

Costs are associated with developing and implementing an effective screening process. However, absent such a process, a bank may incur significant expenses in recruiting, hiring, training and ultimately terminating unqualified individuals.

Sometimes, regulations prohibit any person who has been convicted of a crime involving dishonesty or money laundering from becoming or continuing as an institution-affiliated party; owning or controlling, directly or indirectly, an institution; or otherwise participating, directly or indirectly, in the conduct of the affairs of an institution without the prior written consent of the regulator. Consultants who take part in the affairs of a financial institution may be subject to this requirement too.

Therefore, pre-employment background screening should be established by all financial institutions that, at a minimum, reveals information regarding a job applicant's criminal convictions. Sometimes, the level of screening should be raised. The sensitivity of the position or the access level of an individual employee may warrant additional background screening, which should include verification of references, experience, education and professional qualifications, according to the FDIC.

Furthermore, just as management verifies the identity of customers, it should verify the identity of job applicants. Once the person is hired, an ongoing approach to screening should be considered for specific positions, as circumstances change, or as needed for a comprehensive review of departmental staff over a period of time. Management should also have policies that address what to do when a screening uncovers information contrary to what the applicant or employee provided, according to the FDIC.



An institution may perform fingerprint checks periodically for employees in sensitive positions, or it may contract with a vendor to conduct an extensive background check when the employee is being considered for promotion to a high-level position. Without such screening procedures in place, financial institutions risk running afoul of the prohibition against employing statutorily disqualified individuals. The extent of the screening depends on the circumstances, with reasonableness being the standard.

#### Real Life Case

The Bank of New York case speaks volumes about the vulnerability of financial institutions to the problems that their own employees can cause. Lucy Edwards, a vice president of BONY's Eastern European Division, introduced her husband, Peter Berlin, to the bank. In 1996, Berlin opened two accounts at BONY for Benex International Co. Inc., and BECS International L.L.C., which he controlled and in which Edwards had an undisclosed interest. In 1998, Berlin opened another account at BONY for Lowland Inc., which he also controlled. Combined, the three companies deposited more than \$7 billion at BONY in a 42-month period and transmitted nearly all the funds shortly afterwards to offshore locations at the request of Russian banks and other customers who were evading Russian taxes, duties and other government requirements. The three Berlin companies had no commercial purpose. Their only function was to receive wire transfers from Russian banks and other customers, deposit the money in the BONY accounts and transmit the money to offshore accounts or suppliers of the Russian customers. Benex, BECS and Lowland, all of which had offices in BONY's primary service area, were not registered under New York law as money transmitters. In addition, the New York mailing address for Benex and BECS was the office of Torfinex, another unlicensed money transmitter controlled by a Russian bank that was under indictment in Russia. Since 1992, it has been a federal crime in the United States to

conduct a money transmitting business without a state license (Title 18, USC Sec. 1960).

Using a shell bank registered in the South Pacific island of Nauru, a well-known money laundering haven, more than \$3 billion in wire transfers flowed through the correspondent accounts of two Russian banks at BONY to the Benex and BECS accounts. The Russian customers that Berlin and Edwards served told BONY that the Nauru shell bank had offices in Australia and New Jersey, which was not true. In a 41-month period, Berlin and Edwards received about \$1.8 million in commissions from their Russian customers for the funds deposited in the Benex, BECS and Lowland accounts at BONY. These amounts were paid through accounts at BONY in the name of Benex, a Russian company and a Russian correspondent bank of BONY. Berlin and Edwards pled guilty to money laundering, among other charges, were fined, were required to make restitution and received a suspended sentence.

## SUSPICIOUS OR UNUSUAL TRANSACTION MONITORING AND REPORTING

---

Proper due diligence may require management to gather further information regarding a customer or his transaction before deeming it suspicious and deciding to report it as part of a compliance program. While there are no hard and fast rules as to what constitutes suspicious activity, financial institution employees should watch for activity that is not consistent with a customer's source of income or regular business.

Because financial institutions must sort through thousands of transactions each day, a firm's system for monitoring and reporting suspicious activity should be risk-based, and should be determined by factors such as the firm's size, the nature of its business, its

location, frequency and size of transactions and the types and geographical location of its customers.

Many financial institutions create internal reports that can be used to discover possible money laundering and terrorist financing. Some of the reports include:

- Daily cash activity in excess of the country's reporting threshold.
- Daily cash activity just below the country's reporting threshold (to identify possible structuring).
- Cash activity aggregated over a period of time (e.g., individual transactions over a certain amount, or totaling more than a certain amount over a 30-day period) to identify possible structuring.
- Wire transfer reports/logs (with filters using amount and geographical factors).
- Monetary instrument logs/reports.
- Check kiting/drawing on uncollected funds (significant debit/credit flows).
- Significant change reports.
- New account activity reports.

While reporting procedures vary from country to country, a typical suspicious or unusual transaction reporting process within a financial institution includes:

- Procedures to identify potential suspicious transactions or activity.
- A formal evaluation of each instance, and continuation, of unusual transactions or activity.
- Documentation of the suspicious transaction reporting decision, whether or not filed with the authorities.
- Procedures to periodically notify senior management or the board of directors of suspicious transaction filings.

- Employee training on detecting suspicious transactions or activity.

Most countries that require suspicious transaction reporting prohibit disclosing the filing to the subject of the report.

Most laws also provide immunity from civil liability to the filing institution and its employees.

Good recordkeeping procedures are a key to managing any regulatory or legal implications of the filing. National laws or regulations usually dictate the length of time financial institutions and businesses must maintain records, the types of records that must be on hand and how they must be provided to regulatory or law enforcement personnel upon request.

There is no international clearinghouse for keeping STRs, but Financial Intelligence Units in various countries often publish reports on how many STRs are filed each year, which areas are filing the most reports and what the suspicious activity trends are. This information can be shared country to country through agreements the FIUs sign with each other.

## RED FLAGS OR INDICATORS OF MONEY LAUNDERING

---

While there is no exhaustive list of tried-and-true suspicious activity indicators for businesses, there are many common indicators of financial crime and money laundering activity that your institution can be ready for.

One expert, Michael Kelsey, who has more than 25 years experience in bank compliance and has taught banking and AML at Widener University School of Law and the University of Delaware, says financial institutions should look out for suspicious trends that might be caught by other systems already in place, including:

- **ATM Usage:** The convenience of ATMs makes them ideal financial services delivery points for launderers and terrorists. Launderers can use an account in the U.S. to deposit funds within the U.S. and have another person withdraw them outside the country. Domestic terrorists might find ATMs convenient to access accounts as they travel. Deposit accounts with multiple access devices might be indicators of illegal abuse of ATMs. Institutions should consider analyzing their data to identify multinational transactions via ATMs.
- **Moving Customers:** A customer who moves frequently could be suspicious, particularly if there is nothing in that person's information suggesting that frequent changes in residence is normal.
- **Opening Deposits or Investments:** In addition to asking new customers about sources of funds, when appropriate, institutions should consider determining the background of customer's first transaction. Of particular interest would be a wire transfer from outside the country, monetary instruments and, of course, large cash transactions.
- **Out-of-Market Windfalls:** If you think a customer who just appeared at your institution sounds too good to be true, you might be right. Pay attention to one whose address is far from your institution, especially if there is no special reason why you are to receive the business. If the customer is a business, the distance to its operations may be an attempt to prevent you from verifying that there is no legitimate business after all. Do not be persuaded by sales personnel who might follow a "no questions asked" philosophy of taking in new business.
- **Credit balances:** Customers may "over pay" on their credit line or card accounts prior to vacations or when other circumstances may prevent them from making payments, or when they anticipate numerous upcoming transactions. But large or

frequent credit balances may also be red flags for money laundering. Institutions should consider periodic evaluation of their credit products for unusual overpayments.

- **Common addresses, phone numbers, IP addresses and other data:** While household members often bank at the same institution, unrelated customers who share street or IP addresses, or who have the same phone number or email account, could be using their accounts for suspicious or fraudulent purposes. Customers who change their information after opening their accounts to common locations may be especially suspicious. Institutions should consider evaluation of customers who have these common data characteristics.

These are just some factors an institution can use to identify high-risk accounts that merit closer scrutiny. Look for ways your anti-money laundering program can be ready for these activities and can potentially thwart them before they occur.

Methods of money laundering have become more sophisticated as the complexity of financial relationships has grown and paths through which funds move worldwide through financial institutions have multiplied.

In the October 2005 issue of FinCEN's "SAR Activity Review — Trends, Tips and Issues," money laundering indicators in a securities broker-dealer setting were discussed. One was the intentional abuse of accounts, reflecting individuals trying to use brokerage accounts in a manner inconsistent with the stated investment objective.

#### Example

The predominant activity reported in this category was funding an account, but allowing the money to remain idle. Because some investment accounts do not bear interest, failure to invest assets is actually considered a loss in most cases. Therefore, lack of activity in an investment account may serve as a red flag to broker-

dealers. The decision to file a Suspicious Transaction Report usually is made after long periods of inactivity followed by a sudden liquidation of the account, through check writing, debit card use at ATMs, and outbound fund transfers, without obvious economic benefit. Excessive outbound wire activity was common in Suspicious Transaction Reports (STRs) filed by the securities and futures industries. Preliminary indicators are that individuals who engage in this activity within one year of establishing a brokerage account were more likely to send funds abroad. Several filers near the Canadian or Mexican borders reported strong suspicions that funds in idle brokerage accounts were being wired to foreign institutions in Canada and Mexico to evade taxes.

## SUSPICIOUS CUSTOMER BEHAVIOR

---

The following situations may indicate money laundering. These lists are not exhaustive, but may be helpful.

- Customer has an unusual or excessively nervous demeanor.
- Customer discusses your record-keeping or reporting requirements with the apparent intention of avoiding them.
- Customer threatens an employee in an effort to discourage required recordkeeping or reporting.
- Customer is reluctant to proceed with a transaction after being told it must be reported.
- Customer suggests paying a gratuity to an employee.
- Customer appears to have a hidden agenda or behaves abnormally, such as turning down the chance to obtain a higher interest rate on a large account balance.

- Customer, who is a public official, opens account in the name of a family member who begins making large deposits not consistent with the known sources of legitimate family income.
- Customer makes large cash deposit without having counted the cash.
- Customer frequently exchanges small bills for large bills.
- Customer's cash deposits often contain counterfeit bills or musty or extremely dirty bills.
- Customer, who is a student, uncharacteristically transfers or exchanges large sums of money.
- Account shows high velocity in the movement of funds, but maintains low beginning and ending daily balances.
- Transaction involves offshore institutions whose names resemble those of well-known legitimate financial institutions.
- Transaction involves unfamiliar countries or islands that are hard to find on an atlas or map.
- Agent, attorney or financial advisor acts for another person without proper documentation, such as a power of attorney.
- Customer indulges in foreign exchange transactions/ currency swaps without caring about the margins.
- Customer submits account documentation showing an unclear ownership structure.

### SUSPICIOUS CUSTOMER IDENTIFICATION CIRCUMSTANCES

---

- Customer furnishes unusual or suspicious identification documents or declines to produce originals for verification.



- Customer is unwilling to provide personal background information when opening an account.
- Customer tries to open an account without identification, references or complete local address.
- Customer's permanent address is outside of the institution's service area.
- Customer's home or business telephone is disconnected.
- Customer does not wish a statement of his account or any mail sent to him.
- Customer asks many questions about how the financial institution disseminates information about the identification of its customers.
- A business customer is reluctant to reveal details about the business activities or to provide financial statements or documents about a related business entity.
- Customer provides no record of past or present employment on a loan application.
- Customer claims to be a law enforcement agent conducting an undercover operation when there are no valid indicators to support that claim.

## SUSPICIOUS CASH TRANSACTIONS

---

- Customer comes in with another customer and they go to different tellers to conduct currency transactions under the reporting threshold.
- Customer makes large cash deposit containing many larger denomination bills.

- Customer opens several accounts in one or more names, and then makes several cash deposits under the reporting threshold.
- Customer withdraws cash in amounts under the reporting threshold.
- Customer withdraws cash from one of his accounts and deposits the cash into another account the customer owns.
- Customer conducts unusual cash transactions through night deposit boxes, especially large sums that are not consistent with the customer's business.
- Customer makes frequent deposits or withdrawals of large amounts of currency for no apparent business reason, or for a business that generally does not generate large amounts of cash.
- Customer conducts large cash transactions at different branches on the same day, or coordinates others to do so in his behalf.
- Customer deposits cash into several accounts in amounts below the reporting threshold and then consolidates the funds into one account and wire transfers them abroad.
- Customer attempts to take back a portion of a cash deposit that exceeds the reporting threshold after learning that a currency transaction report will otherwise be filed.
- Customer conducts several cash deposits below the reporting threshold at ATMs.
- Corporate account has deposits or withdrawals primarily in cash, rather than checks.
- Customer frequently deposits large sums of cash wrapped in currency straps.

- Customer makes frequent purchases of monetary instruments with cash in amounts less than the reporting threshold.
- Customer conducts an unusual number of foreign currency exchange transactions.

### SUSPICIOUS NON-CASH DEPOSITS

---

- Customer deposits a large number of traveler's checks, often in the same denominations and in sequence.
- Customer deposits large numbers of consecutively numbered money orders.
- Customer deposits checks and/or money orders that are not consistent with the stated purpose of the account or nature of business.
- Customer deposits a large number of third party checks.
- Funds withdrawn from the accounts are not consistent with the normal business or personal activity of the account holder or include transfers to suspicious international jurisdictions.
- Funds deposited are moved quickly out of the account via payment methods inconsistent with the established purpose of the account.

### SUSPICIOUS WIRE TRANSFER TRANSACTIONS

---

- Non-accountholder sends wire transfer with funds that include numerous monetary instruments, each in an amount under the reporting threshold.
- An incoming wire transfer has instructions to convert the funds to cashier's checks and to mail them to a non-accountholder.

- A wire transfer directs large sums to secrecy havens.
- An incoming wire transfer, followed by an immediate purchase by the beneficiary of monetary instruments for payment to another party.
- An increase in international wire transfer activity in an account with no history of such activity or where the stated business of the customer does not warrant it.
- Customer frequently shifts purported international profits by wire transfer out of the country.
- Customer receives many small incoming wire transfers and then orders a large outgoing wire transfer to another country.
- Customer deposits bearer instruments followed by instructions to wire the funds to a third party.
- Account in the name of a currency exchange house receives wire transfers or cash deposits under the reporting threshold.

### SUSPICIOUS SAFE DEPOSIT BOX ACTIVITY

---

- Customer spends an unusual amount of time in the safe deposit box area, possibly indicating the safekeeping of large amounts of cash.
- Customer often visits the safe deposit box area immediately before making cash deposits of sums under the reporting threshold.
- Customer rents multiple safe deposit boxes.

### SUSPICIOUS ACTIVITY IN CREDIT TRANSACTIONS

---

- A customer's financial statement makes representations that do not conform to accounting principles.

- A transaction is made to appear more complicated than it needs to be by use of impressive but nonsensical terms such as emission rate, prime bank notes, standby commitment, arbitrage or hedge contracts.
- Customer requests loans either made to offshore companies or secured by obligations of offshore banks.
- Customer suddenly pays off a large problem loan with no plausible explanation as to the source of funds.
- Customer purchases certificates of deposit and uses them as collateral for a loan.
- Customer collateralizes a loan with cash deposits.
- Customer uses cash collateral located offshore to obtain a loan.
- Customer's loan proceeds are unexpectedly transferred offshore.

### SUSPICIOUS COMMERCIAL ACCOUNT ACTIVITY

---

- Business customer presents financial statements noticeably different from those of similar businesses.
- Large business presents financial statements that are not prepared by an accountant.
- Retail business that provides check-cashing services does not make withdrawals of cash against check deposits, possibly indicating that it has another source of cash.
- Customer maintains an inordinately large number of accounts for the type of business purportedly being conducted.
- Corporate account shows little or no regular, periodic activity.

- A transaction includes circumstances that would cause a banker to reject a loan application because of doubts about the collateral.

## SUSPICIOUS TRADE FINANCING TRANSACTIONS

---

- Customer seeks trade financing on the export or import of commodities whose stated prices are substantially more or less than those in a similar market situation or environment.
- Customer makes changes to a letter of credit beneficiary just before payment is to be made.
- Customer changes the place of payment in a letter of credit to an account in a country other than the beneficiary's stated location.
- Customer's standby letter of credit is used as a bid or performance bond without the normal reference to an underlying project or contract, or designates unusual beneficiaries.
- Letter of Credit is inconsistent with customer's business.
- Letter of Credit covers goods that have little demand in importer's country.
- Letter of Credit covers goods that are rarely if ever produced in the exporter's country.
- Documents arrive without title documents.
- Letter of Credit is received from countries with a high risk for money laundering.
- Commodities are shipped through one or more jurisdictions for no apparent economic or logistical reason.

- Transaction involves the use of repeatedly amended or frequently extended letters of credit.
- Size of the shipment appears inconsistent with the regular volume of business of the importer or of the exporter.

### SUSPICIOUS INVESTMENT ACTIVITY

---

- Customer uses an investment account as a pass-through vehicle to wire funds to off-shore locations.
- Investor seems uninterested in the usual decisions to be made about investment accounts, such as fees or the suitability of the investment vehicles.
- Customer wants to liquidate a large position through a series of small transactions.
- Customer deposits cash, money orders, traveler's checks or cashier's checks in amounts under the reporting threshold to fund an investment account.
- Customer cashes out annuities during the "free look" period or surrenders the annuities early.

### SUSPICIOUS EMPLOYEE ACTIVITY

---

- Employee exaggerates the credentials, background or financial ability and resources of a customer in written reports the bank requires.
- Employee is involved in an excessive number of unresolved exceptions.
- Employee lives a lavish lifestyle that could not be supported by his or her salary.
- Employee frequently overrides internal controls or established approval authority or circumvents policy.

- Employee uses company resources to further private interests.
- Employee assists transactions where the identity of the ultimate beneficiary or counter party is undisclosed.
- Employee avoids taking periodic vacations.

### SUSPICIOUS ACTIVITY IN A MONEY REMITTER/ CURRENCY EXCHANGE HOUSE SETTING

---

- Unusual use of money orders, traveler's checks or funds transfers.
- Two or more persons working together in transactions.
- Transaction altered to avoid filing a Currency Transaction Report (CTR).
- Customer comes in frequently to purchase less than \$3,000 in instruments each time (or the local threshold).
- Transaction altered to avoid completion of record of funds transfer, money order or traveler's checks of \$3,000 or more (or the local threshold).
- Same person uses multiple locations in a short time period.
- Two or more persons use the same identification.
- One person uses multiple identification documents.

### SUSPICIOUS ACTIVITY IN AN INSURANCE COMPANY SETTING

---

- Cash payments on insurance policies.
- Refunds requested during a policy's "legal cancellation period."



- Policy premiums paid from abroad, especially from an offshore financial center.
- A policy calling for the periodic payment of premiums in large amounts.
- Changing the named beneficiary of a policy to a person with no clear relationship to the policyholder.
- Lack of concern for significant tax or other penalties assessed when canceling a policy.
- Redemption of insurance bonds originally subscribed to by an individual in one country by a business entity in another country.

### SUSPICIOUS ACTIVITY IN A BROKER-DEALER SETTING

---

In 2002, the U.S. National Association of Securities Dealers (NASD), a self-regulatory organization that oversees the NASDAQ Stock Market under the authority of the U.S. Securities and Exchange Commission, offered in its “Special NASD Notice to Members” signs of suspicious activity to the securities field:

- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information, or is otherwise evasive regarding that person or entity.
- For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.
- The customer’s account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity.
- The customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer the proceeds from the account.

- The customer engages in excessive journal entries between unrelated accounts without any apparent business purpose.
- The customer requests that a transaction be processed in such a manner so as to avoid the firm's normal documentation requirements.
- The customer, for no apparent reason or in conjunction with other "red flags," engages in transactions involving certain types of securities, such as penny stocks, Regulation "S" (Reg S) stocks, and bearer bonds, which, although legitimate, have been used in connection with fraudulent schemes and money laundering activity. (Such transactions may warrant further due diligence.)
- The customer's account shows an unexplained high level of activity with very low levels of securities transactions.

### SUSPICIOUS ACTIVITY INDICATORS OF BLACK MARKET PESO EXCHANGE MONEY LAUNDERING METHOD

---

A 1999 U.S. Customs "trade advisory" titled "The Black Market Peso Exchange" to businesses dealing in Latin America described the mechanics of the BMPE and provided guidance on reporting suspected laundering activity. The advisory describes these "red flags" as indicators of BMPE:

- Payment made in cash by a third party with no connection to the underlying transaction.
- Payment made by wire transfers from third parties unconnected to the underlying transaction.
- Payment made with checks, bank drafts or money orders not drawn on the account of the purchaser.

A 1997 FinCEN advisory offered financial institutions these “potential indicators” that an institution or business is being abused by peso brokers:

- Structured currency deposits to individual checking accounts with multiple daily deposits to multiple accounts at different branches of the same bank on the same day.
- Consumer checking accounts which are used for a period of time and then become dormant.
- Personal checking accounts opened by foreign nationals who come to the bank together.
- Multiple accounts opened on the same day or held by the same foreign nationals at various banks.
- Increases in the frequency or amounts of currency deposits by U.S. business account holders who export to Colombia.

## ELECTRONIC ANTI-MONEY LAUNDERING SOLUTIONS

---

Many financial institutions would agree that anti-money laundering compliance is nearly impossible without some help from technology. The sheer number of people and the volume of regulations and data involved in complying with regulations make manual compliance difficult if not impossible. Many institutions have computer systems to automate their compliance activities, while a few still undertake their efforts manually.

Although technology forms one of a number of components in an overall AML solution, good technology will equip organizations with improved defenses in the fight against financial crime by providing:

- Transaction monitoring: scanning and analyzing data for potential money laundering activity.

- Watch list filtering: screening new accounts, existing customers, beneficiaries and transaction counterparties against terrorist, criminal and other blocked-persons watch lists.
- Automation of regulatory reporting: filing suspicious transaction reports (STRs), currency transaction reports (CTRs), or other regulatory reports with the government.
- A detailed audit trail: demonstrates compliance efforts to regulators.

Many software companies can sell an institution dedicated systems to combat laundering, while some organizations have internally generated electronic systems. Before designing your AML compliance program or purchasing new technology, review the feasibility, costs and benefits to be derived from each course of action.

Here are some ways financial institutions use technology that is already in place to assist them in their AML goals:

- Profiling system;
- Large cash transaction reporting;
- Recordkeeping;
- Background checks;
- Corporate “hot file”;
- Case management tracking system; and
- Incident reporting database.

Some financial institutions choose to take the plunge and opt for anti-money laundering software packages. Many will use a Request For Proposal (RFP) method. The institution will send out RFPs to software providers that it believes may be qualified to participate. An RFP lists project specifications and application procedures. The objective of the RFP is to select a system that

may assist the institution in completing its responsibilities under applicable money laundering regulations. The system(s) may help identify potentially high-risk customers, accounts and transactions and may aid in conducting, managing, documenting any resulting investigations, as well as streamlining the completion and filing of any required STRs.

Most institutions seek a partner with a longstanding commitment to stay ahead of the rapidly changing regulatory landscape and with a track record that reflects flexibility, agility and urgency in delivering features that improve clients' efficiency in monitoring the right transactions and investigating the right clients. Ideally, the system must be flexible, fast and efficient to deploy over multiple branches. It should allow the institution to navigate seamlessly around client relationships, accounts, and transactions across a variety of product lines and systems, including deposits, wires, loans, trust, brokerage, letters of credit and check imaging applications. A single view into clients' relationships is of paramount importance in delivering efficient, reliable and instant access to information. Each institution will have to identify the vendor that best meets its needs. During the RFP process, most institutions form evaluation teams composed of management from compliance, operations, technology and business. The team, facilitated by the project manager, will be responsible for reviewing and scoring all responses to the RFP.

Which automated tool is right for your organization? Each case will be different, depending on customer base, size and services offered. In general, however, if your organization decides to buy software, look for these functional components:

- Ability to monitor transactions and identify anomalies that might indicate suspicious activity.
- Ability to gather CDD information for new and existing customers, score customer responses and store CDD data for subsequent use.
- Ability to conduct advanced evaluation and analysis of suspicious/unusual transactions identified by the

monitoring system in the context of each client's risk profile and that of their peer group.

- Ability to view individual alerts within the broader context of the client's total activity at the institution.
- Workflow features, including the ability to create a case from an alert or series of alerts, and collaboration (simultaneous or serial) among multiple interested parties to view and update information, and the ability to share AML-related information across monitoring and investigating units and throughout the bank as needed.
- Ability to use data from the institution's core customer and transaction systems and databases to inform/update monitoring and case management activities.
- Ability to store and recall at least 12 months' data for trend analysis.
- Ability to manage the assignment, routing, approval and ongoing monitoring of suspicious activity investigations.
- Automated preparation and filing of STRs to the financial intelligence unit.
- Standard and ad-hoc reporting on the nature and volume of suspicious activity investigations and investigator productivity for management and other audiences.
- Enhanced ability to plan, assign and monitor the caseload per employee of AML-related investigations.
- Ability to provide comprehensive and accurate reporting of all aspects of AML compliance, including reporting to management, reporting to regulators, productivity reporting and ad-hoc reporting.
- User-friendly updating of risk-parameter settings without need for special technical computing skills.

In addition to these functionalities, evaluate the following aspects:

- Ease of use of the application, as well as the configuration of new and changed transaction monitoring rules.
- Ease of data integration, system implementation and configuration.
- Scalability of application – the ability of the system to grow with the institution.
- Extent to which the system(s) can be supported with internal resources.
- User satisfaction with hardware and software support.
- Price, including initial cost, ongoing costs to sustain the system or to expand the capabilities of the system, both in terms of what the vendor will charge and how much the institution will need to spend in terms of dollars, personnel and technology capacity.

In addition to providing possible regulatory compliance solutions, automated tools may help an institution analyze how customers and users are using its products and services. For marketing purposes, patterns of activity among types of clients and different business lines can also be represented by graphs and statistical reports. Depending on an institution's needs, a variety of software products can automate these tasks — from the more standard analytical systems to sophisticated artificial intelligence.

Automated tools may also help with documentation management, which can be a large burden for many institutions. Historically, imaging systems offered quick and paperless access to records. Convenience is not enough anymore, and technology has gone one step further. New systems can track and report the status of all documents, including those that are missing or expired. One-stop access systems can provide images as well as standardization and control for documents that must be accounted for and produced for compliance purposes.

Automation is used for more than increased efficiency and control. It also may reflect a company's commitment to meet or exceed compliance requirements. A byproduct of this commitment is that regulators can receive prompt, concise and formatted information.

## SUMMARY

---

An institution's commitment to play its part in preventing money laundering is shown in a sound AML program, demonstrating compliance with both the letter and spirit of requirements imposed by laws and regulations.

Many regulators now require that financial institutions have systems and controls in place that are commensurate with their specific risks of being used for money laundering and terrorist financing. Assessing your institution's money laundering risks is one of the most important steps in creating a good AML program. The program should be consistent with the risks associated with the institution's customer base, location, size and the products and services it offers.

Designing and structuring these programs should be top priorities. Implementation and maintenance of the program is equally important. These steps must be undertaken with a clear view of what the legal requirements are in the jurisdiction where the financial institution or business is located, and what the internal policies and specific vulnerabilities of the entity are.

This section illustrated what to consider when designing a compliance program, how to spot, manage, document and follow up on suspicious activities, how to maintain your program effectively and efficiently, and what you need to know about properly training and screening employees who use the system.



## REVIEW QUESTIONS

---

- What are the key elements of a customer identification program?
- What is risk-scoring, and what are the factors that determine the risk for a product or customer?
- What are the indicators of money laundering in a broker-dealer setting?
- What are the elements to consider when selecting money laundering monitoring software?
- You spot a long-time colleague at work conducting a transaction you know is considered suspicious. It is never reported. How should you handle the situation?

