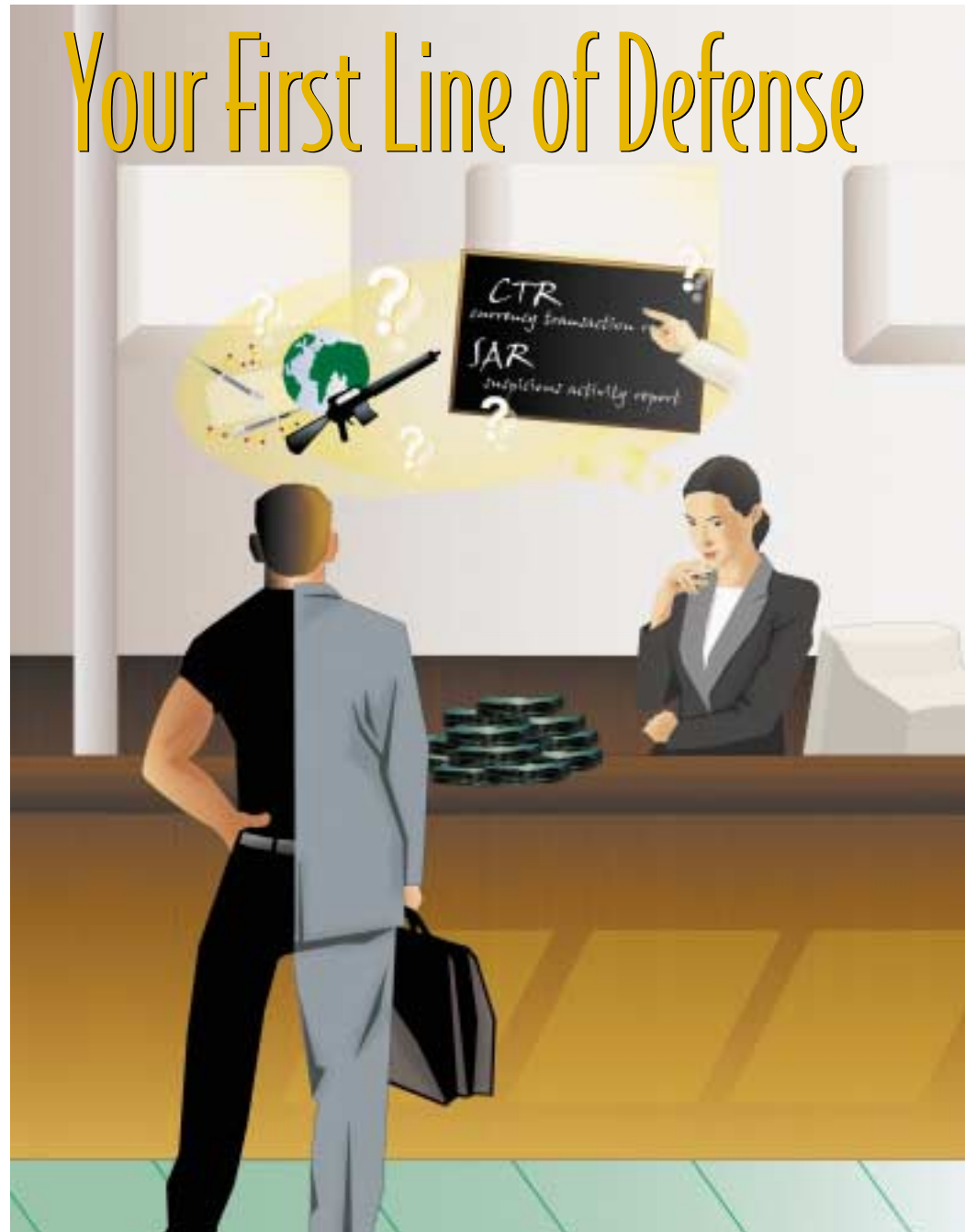


AML Training for Staff:

While it is not necessary for everyone at your institution to know every detail of anti-money laundering laws, a general understanding of the laws and regulations helps put the requirements in perspective and emphasizes the importance of complying. This article will provide ideas for training your staff to comply with the laws and to prevent your institution from being used as a conduit for money laundering. This training kit is designed so that you can customize the lessons to meet your institution's training needs.



by Betsy Fredrickson and Shannon Bennett

In this post-September 11 world, detecting and preventing money laundering and terrorist financing is more important than ever. It is crucial that your employees understand their role in protecting your institution from being used to facilitate illegal activity. This is true for all employees — whether they are executives, have customer contact, see customer transaction activity, or handle cash.

Since the 1970s, many laws and regulations have been enacted and amended to help deter money laundering. The main laws are the Bank Secrecy Act (which was recently fortified by the USA PATRIOT Act) and the Money Laundering Control Act.

The goal of anti-money laundering (AML) training is to have your staff be able to do the following:

- understand money laundering and terrorist financing;
- comply by knowing when and how to use the required forms;
- prevent money laundering and terrorist financing by identifying suspicious behaviors; and
- report suspicious activity to the proper authorities.

Lesson A: Basic Information Employees Should Understand

While the laws and procedures surrounding money laundering and terrorist financing are of primary importance

to your institution, it is good to start your training by providing a basic understanding of the criminal activities themselves. Having your staff interact with you during the training is important, as it allows them to put the topic in perspective.

Start your meeting by asking the following questions and asking participants to help develop the answers:

■ **What is money laundering?** Money laundering is a method used to “wash” away the paper trail of illegally obtained funds in order to conceal the true ownership and source of the funds.

■ **Is money laundering a crime?** Yes, although money laundering itself did not become a crime until the Money Laundering Control Act of 1986 was passed. Since then, the laws and activities surrounding the “business” of money laundering have been continually changing.

■ **What recent events have made the prevention of money laundering a top priority?** The September 11 terrorist attacks and the ongoing threat of terrorist activity.

■ **Why would the September 11 attacks be associated with money laundering?** Money laundering is often associated with terrorism. It is one of the ways terrorists finance their activities. Since the attacks, the prevention of terrorist financing is of enormous importance both to our nation and to the reputation of financial institutions. Terrorist financing has recently been added as an offense in the anti-money laundering laws.

■ **Why does there seem to be a distinction between money laundering**

and terrorist financing? Terrorist financing differs from typical money laundering in that funds may have a legitimate source and they are often used to finance day-to-day operations and living expenses. As with typical money laundering, the people involved do not want the funds to be traced back to them. Thus, the behaviors you are watching for will probably be similar.

■ **Just for fun — a story to share.** Criminals have sought to put distance between themselves and the profits from illegal activity since the early days of organized crime. Criminals like Al Capone established front businesses, such as laundries, as a way to legitimize and disguise money they obtained from the illegal sale of alcohol and other illegal activities, such as gambling. Because the illegal activity usually generated payment in coins, businesses such as laundries created a legitimate explanation for the funds obtained through the illegal activities. This is where the term “money laundering” originated.

■ **Fun trivia question:** If money laundering wasn’t a crime during Prohibition, why did Al Capone go to jail? Answer: Tax evasion.

Lesson B: The Ins and Outs of Money Laundering

During this lesson, draw a chart of the methods used to launder money on a dry-erase board or flip chart. After explaining how money laundering occurs, ask for a list of examples to place under each

Editor’s Note: Instructions to trainers are shown as *italicized copy* throughout (excluding headings).

stage. This will allow your employees to visualize the stages that would affect them the most.

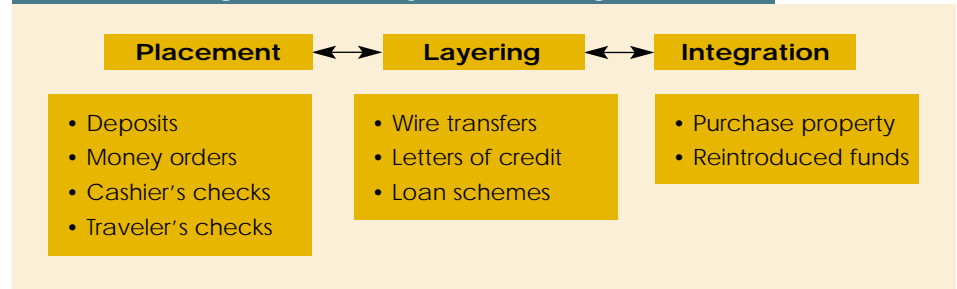
■ How is money laundering done?

Money laundering is the process of converting cash from criminal activity into a form that can be easily exchanged without tracing it back to its original origin. This process makes the money appear legitimate. There are three stages of money laundering that occur independently or simultaneously (see Exhibit 1):

- **Placement:** placing funds into the system by deposits or other means. For instance, purchasing monetary instruments or depositing illegal funds directly into an account. (Due to the amounts of cash, this is often the easiest stage at which to detect money laundering.)
- **Layering:** separating the funds from the illegal activity by layering them into the system with complex transactions — for instance, wiring funds to another account.
- **Integration:** creating the appearance of legitimate funds by the use of additional transactions. For instance, investing the laundered funds by purchasing real estate or other property to give the appearance of legitimacy.

The following example may help participants understand the big picture: A drug dealer who has acquired mountains of cash after a few days of selling drugs has a problem. He has no legitimate explanation for the cash. It is not very secure. It is difficult to move around and he needs to find a way to buy more drugs to sell. Typically, the drug dealer will move the money to a counting house where it

Exhibit 1: Stages of Money Laundering



will be broken up into smaller amounts, each of which will likely be less than the \$10,000 reporting requirement. The currency may then be converted to bank checks that are deposited into different banks in smaller amounts (placement). Then, the money may be moved around by wire transfer through different countries or jurisdictions, be converted into certificates of deposit (CDs), and used as collateral for a loan (layering). The loan proceeds could then be transferred to the drug trafficker without a direct connection (integration).

■ When does money laundering usually occur? Ask participants for their thoughts. Money laundering usually happens from three to six months after the account has been established. However, keep in mind that long-term customers can become involved with suspicious activities, too. In addition, do not discount the fact that a less sophisticated criminal may try to use the account for illegal activity immediately.

■ Who does it and why? Create the lists in Exhibit 2 on a dry erase board or flip chart. Ask the following questions:

1. Can we put a face to the person(s) that launders money? If so, give me a list of individuals or organizations that launder money. *Most likely you will get a similar version of the first list in Ex-*

hibit 2. Now create list two and fill in the examples.

The face of a money launderer belongs to anyone who either benefits from the activity or is just involved in helping launder the money, which may include lawyers, accountants, other professionals, and even bank employees.

Train employees to focus on the behavior, rather than the physical description of an individual. This will teach them to tune into suspicious activity instead of focusing on certain individuals.

2. If the goal of money laundering is to disguise the source of the funds, let's develop a list of reasons why they do it? *Answers include tax evasion, to fund terrorist activities, to hide illegal activities, and bribery.*

Have the class discuss answers to the following questions:

■ What institutions are likely to be targeted? Historically, larger financial institutions in metropolitan areas were more often the targets for those wanting to launder money.

■ Why would financial institutions in metro areas be the prime choice for criminals? High volumes of customers and the ability to conduct multiple

transactions at different branches can make unusual activity more likely to go unnoticed at larger institutions.

■ **So why would the criminals now be targeting smaller institutions?** Because larger financial institutions have invested in software to identify suspicious activity, the criminals are now focusing on smaller institutions, which are less likely to have sophisticated systems to detect illegal activity.

■ **Does this mean that large institutions are no longer vulnerable?** No, this doesn't mean the large metro institutions are off the hook. They are still very appealing because of their international nature. It simply means that all financial institutions, regardless of their size or region of the United States, are vulnerable.

Discuss the likelihood of your institution being targeted.

■ **What happens if an employee or an institution does not comply with the anti-money laundering laws?** Because the consequences of not following anti-money laundering laws and institution policies are very severe, it is very important to explain the penalties to your staff (see Exhibit 3). Another important point is that any property con-

nected with a laundered transaction, including loan collateral, may be forfeited. This is true even if money is commingled and not all of the money involved can be traced to the illegal activity (or terrorist financing).

Lesson C: Forms, Reporting Requirements, and Exemptions

The major regulatory reporting forms used by financial institutions are important tools to both your institution and the government. They create a paper trail that can help you detect all kinds of illegal activity.

Begin your lesson by providing each employee with a copy of a currency transaction report and start with the following questions and responses. Remember that you should incorporate your institution's procedures surrounding the following forms into your training program.

■ **What is a CTR?** A currency transaction report is a report that all financial institutions must file when a person conducts one or more transactions in a single day that involve, in aggregate, more than \$10,000 of currency.

■ **Why is it important for banks to complete CTRs?** They are important

because they are used to create a paper trail that can help detect and trace all kinds of illegal activity.

An employee should complete a CTR when the dollar amount requirements are met. The form requires basic information concerning who conducted the transaction; on whose behalf it was conducted; and the amount and a description of the transaction.

It is important that employees understand that this requirement applies to transactions in currency. Remind them of the definitions of "currency" and "person."

"Currency" means coins, paper money, bills, or notes. It does not include bank checks, wire transfers, or anything that does not include physical currency. This includes all currency from customer to bank and, separately, all currency from bank to customer. Focus on all currency, no matter which way it is going.

A "person" includes an individual, corporation, partnership, trust, or estate, or any other entity treated as a legal person.

The following training tool includes examples of situations that might occur to help employees decide how to respond to common CTR questions. It also will help prevent common mistakes.

How To Complete a CTR— Common Questions

The CTR instructions can be confusing. Here are some examples to help your employees complete the form. You might want to have your employees have a copy of the CTR in front of them for this exer-

Exhibit 2: Individuals/Organizations that Launder Money

List 1	List 2
<ul style="list-style-type: none">• Drug dealers• Terrorists• Criminals	<ul style="list-style-type: none">• Lawyers• Accountants• Business owners• Bank employees

Exhibit 3: Classification of Attacks

Penalties for an individual:

- Up to 20 years' imprisonment per transaction
- Fines up to \$10,000
- Termination
- Barred from employment in the banking industry

Penalties for an institution:

- Up to \$500,000 per transaction, or two times the transaction amount
- Loss of charter
- Loss of FDIC insurance
- Reputational risk

cise. You, as the trainer, may want to project a CTR on an overhead slide.

■ When do I check “multiple persons?” If more than one individual is present and is involved in conducting the transaction, or if the transaction is conducted on behalf of more than one individual.

Scenario One: Bill and his friend Bob, both bank customers, go to a teller window together while Bill cashes a check written out to him for \$12,000. Bob is just talking with the teller. Should information for both Bill and Bob be in the report?

Answer: No. Just include information on Bill. Bob is just socializing and has no connection to the transaction.

Scenario Two: John and Mary work for the same company. They come into the bank at the same time. Each of them gives the teller a cash deposit for the company. Added together, the cash deposits equal \$11,500. Whose information should be included on the CTR? What if John comes in at 10 a.m. and Mary comes in at 2 p.m.?

Answer: You should enter information on all three “persons.” You will need to check box 1(b). Complete Section B of Part I for John. Complete Section B of

Part I on page 2 for Mary. Complete Section A of Part I for the company. If John comes in at 10 a.m. and Mary at 2 p.m., you should still complete the report. You may not be able to get the information for John because he left before the \$10,000 threshold was met. The institution should make reasonable efforts to obtain the required information. If you cannot obtain all of the information, you should check box D in Section B to indicate that the reason you couldn't obtain the required information was a result of multiple transactions.

Scenario Three: A courier brings in a deposit of \$11,000 in cash. He deposits the cash into various accounts owned by a company. Do you need to include the courier in the report?

Answer: You will need to collect information on the courier and the business.

■ Under what circumstances do I check “multiple transactions”?

Scenario One: Two tellers are talking about the distinctive-looking person who was in the bank earlier that day. One of the tellers states that the man deposited a lot of cash into an account. After further discussion, the two discover that the man deposited \$6,000 in cash in one transaction, and \$5,000 in

the other transaction. Does a CTR need to be completed?

Answer: Yes. The tellers have knowledge that the customer made deposits aggregating over \$10,000 in one business day. Because they probably did not collect all the pertinent information at the time, it might be necessary to search records to fill out the form. The bank should make reasonable efforts to obtain the required information. If you cannot obtain all of the information, you should check box D in Section B to indicate that the reason you couldn't obtain the required information was a result of multiple transactions.

Scenario Two: Julie wants to make two cash deposits — one for \$5,000 into her checking account and the other for \$6,000 into her savings account. The teller obtains all of the required information. Should box D in Section B be checked?

Answer: No. While you should check the multiple transactions box at the top of the form, it is not necessary to check box D in Section B. Even though there are two transactions, you have all the required information.

Person(s) Involved in Transaction(s)

■ On whose behalf is this transaction being conducted? This section must always be completed. It is simple if a person is conducting transactions on his or her own behalf, but beyond that it can get a little tricky.

Scenario One: Al and Tony have a joint account. Al withdraws \$11,000 in cash

for his own use. Do you need to fill out information on both Al and Tony?

Answer: Because the transaction is conducted by Al for Al, you only need to obtain his information, not Tony's.

Scenario Two: Son deposits \$11,000 cash into his mom and dad's joint savings account. Whose information do you need?

Answer: You will need information on all three of them. Son is conducting the transaction. His information goes in Section B. The transaction is conducted on the parents' behalf. Their information will go in Section A (one of them will be listed on page 1, the other on page 2).

Other Questions

■ **Is a post office box a sufficient address?** No. You must obtain the street address, too.

■ **Which of the following are not appropriate descriptions of occupation or profession: manager, retired, salesperson, secretary?** Manager, retired, and salesperson are all insufficient descriptions. Ice arena manager, retired judge, and car salesperson would be sufficient. If you are entering information about a business, you should be specific as well.

■ **Who is conducting the transaction?** This section does not need to be completed if one of the following is true:

- conducted by an armored car service;
- conducted by mail;
- conducted at an ATM or night deposit;
- conducted in multiple transactions under \$10,000 and you don't have all

A SAR is required when an employee knows, suspects, or has reason to suspect the processing of a suspicious transaction, but Suspicious activity can be a pretty vague concept.

the required information to complete the section; or

- conducted on own behalf (the information is already in Section A).

■ **What is the amount and type of transaction?**

Scenario One: Joe Vacationer walks up to the teller window and wants to exchange currency from England, Australia, Mexico, and Italy into U.S. currency. How do you fill in the amount and type of transaction section?

Answer: The first step would be to convert the currency into U.S. dollars to determine an amount. After you have determined that the amount of currency exceeds \$10,000, you would then check Box 29 (foreign currency), and describe the country with the largest amount of currency. For example, if most of the currency Joe is exchanging were in lire, you would write Italy. Then, check the other boxes that apply. In this case, Box 33 (currency exchange) would be checked if all he is doing is exchanging currency. (Remember to write the amount of cash in and the amount of cash out by Boxes 26 and 27 because the amounts are more than \$10,000.)

Scenario Two: How would you complete Box 27 (cash out) if Joe deposited \$8,000 of currency, and just exchanged the other \$3,000?

Answer: You would not need to do anything because the cash out does not meet the \$10,000 threshold.

Exemptions

■ **Why aren't CTRs filled out for _____?** (Insert the name of a business that is exempt at your institution.) Because many legitimate businesses engage in lawful currency transactions that exceed the threshold, the Department of the Treasury allows exemptions for certain persons and for specific transactions and this business has met the exemption requirements.

■ **When can exemptions be granted?** First, there is an automatic exemption for exempt persons — such as government agencies or certain publicly traded corporations. Second, you may exempt specific types of transactions for certain businesses. Certain service providers and certain companies that pay employees in cash can also obtain exemptions if they are established and located in the United States. The third situation occurs when the exemption criteria are not met. In this case you may be able to obtain a special exemption through the Internal Revenue Service.

Suspicious Activity Report (SAR)

■ **When do you fill out a SAR?** A SAR is required when an employee knows, suspects, or has reason to suspect the processing of a suspicious transaction.

■ **What is a suspicious activity?** Suspicious activity can be a pretty vague concept. Generally, it is any conduct that

has no business or apparent lawful purpose, or is not the sort of activity in which the particular customer would normally engage and the institution knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

The following are examples of when a SAR should be filed:

- Agnes notices that a loan officer is diverting \$50 from loans into a separate account. This is insider abuse and should be reported no matter what the amount.
- Joe deposits large amounts of cash under the CTR reporting requirements on a regular basis. This is not consistent with his occupation. The teller becomes suspicious. Because the teller can identify the suspect, this should be reported as soon as the combined amount exceeds \$5,000.
- Frank notifies the bank that there is a \$26,000 cash withdrawal from his money market account that he did not initiate. Even though the bank does not know who was involved in the withdrawal, this should be reported because violations aggregating more than \$25,000 should always be reported.
- Violations aggregating \$5,000 should be reported when money laundering is suspected.

You may have a form similar to a suspicious activity report for employees to fill out before someone else fills out the actual SAR that will be filed. This point in the discussion would be a good time to go

through the procedures surrounding that form with your employees.

Additional SAR information Reminders

■ **Don't tip off the customer.** While the CTR requires that you ask questions, when completing a SAR you cannot tip off the customer. SARs are used in law enforcement investigations and are very valuable in detecting money laundering. Failure to file a SAR as required exposes your institution to civil monetary penalties and/or criminal charges.

■ **Don't be afraid to report.** To allay possible fears, remind your staff that SARs are confidential. If your institution receives a subpoena for the information, it will refuse the subpoena and should notify the Financial Crimes Enforcement Network. It is also important that your employees know there is a safe harbor that protects an institution from any liability to any person arising under state or federal law when the institution reports a suspicious transaction.

Monetary Instrument Record-Keeping Requirement

■ **When do we need to record monetary instruments?** We are required to record any cash purchase of cashier's checks, money orders, bank checks or drafts, or traveler's checks in amounts of \$3,000 to \$10,000. Multiple cash purchases by or for any one person in a single business day for amounts in this range should be recorded as a single transaction if you have knowledge of them.

■ **What is the purpose of the monetary instrument record-keeping requirement?** This form can assist you in de-

tecting structuring. Unlike the currency transaction reporting requirements, there are no exemptions available for this form.

There may be situations where you need to fill out both a CTR and a money instrument report. For example, if a customer presents \$11,000 in cash and deposits \$5,000 into a checking account and uses the remainder to purchase a money order, you would be required to complete both forms.

■ **Other Obligations** Your institution may have other reporting obligations. For instance, you may encounter information sharing requests from the government or from another financial institution. Those obligations usually reside with one person or team at your institution. While they are an important part of your program, they do not need to be covered in your overall training program. However, you will want to discuss the appropriate action if an employee is approached by law enforcement for customer information.

Lesson D: Prevention by Employees

One of the main purposes for training your staff about anti-money laundering activities is to prevent the criminals from getting into the financial system. The more your staff knows about your customers' identity and behaviors, the less likely your institution will become a victim to illegal activities.

Verifying Customer Identity

As part of your AML program, it is important to train your staff on the information that is required by your institution to verify the true identities of all new customers. Verifying a customer's true iden-

tity is critical to preventing and catching any illegal activities in your institution — whether it's money laundering, terrorist financing, or identity theft. Note that this area of your program may be changing in response to the customer identification program (CIP) requirements outlined in Section 326 of the Patriot Act. While you may not have all the details of your program nailed down, the basic requirements for participants are extremely important and should not be overlooked.

A great training technique for this area is to act out an account opening. Have participants get in groups of two. Have one person play the role of account opener and the other the new customer. Provide each team with an application. You can either assign situations to the teams or allow the person playing the new customer to present a difficult situation. For example, here are some challenging identification scenarios:

- The new customer does not drive and cannot provide a driver's license.
- The address on the new customer's identification does not match the address she has given you.
- Two new customers are opening a joint account. One provides identification, the other will not.
- A new business customer wants to open an account. He only has personal identification.

Have the account opener decide what identification and verification methods he or she will need to use consistent with your institution's policy.

Return to a large group and discuss the situations. The resolutions to the scenarios

listed above, or the ones you come up with on your own, will revolve around your institution's policies. Make sure that participants have identified all the required identification and verification processes to satisfy the relevant laws and regulations. Did they get name(s)? street address(es)? Mailing address(es)? Phone number(s)? Identification number(s)? What support- ing documentation did they collect?

Identifying Normal Behavior

Start this part of the training with the following statements and activities to stress the importance of the role your customer contact employees play in preventing suspicious activities:

- One of the main purposes of anti-money laundering training is to prevent criminals from using the financial system to launder money or fund terrorist activity.
- As employees who have contact with our customers you are this institution's best line of defense when it comes to identifying suspicious activities. The more you know about customers' identities and behaviors, the less likely our institution will be a victim of illegal activities.
- Because there may be a problem identifying suspicious activity when a customer has not established a long-term relationship, let's take the time to discuss normal activity for certain businesses and individuals before we discuss suspicious activity.

Write the list of normal behaviors on a dry-erase board or a flip chart, or give staff a handout. Take time to discuss the normal behaviors. Are there others you or your staff can add?

■ Individuals.

- Residence or place of employment is in close proximity to the institution.
- Transactions appear to be consistent with the customer's transaction history.
- Individual has legitimate reason for having others complete transactions — elderly, disabled, or travels for work.

Transactions are similar in amounts and types of deposits with customers in similar occupations (i.e., the deposits of a person who works at a restaurant will often consist of small denominations of currency and coin).

■ Entities.

- Location of the institution is convenient for the business.
- Transactions appear to be consistent with the business' transaction history.
- Individuals conducting transactions on behalf of the business are authorized to do business.

Transactions are consistent with other similar businesses (i.e., mail-order companies' deposits may often consist of numerous money orders).

■ Ongoing Training Tip. To get employees, such as tellers, acquainted with new customers, you may want to share some of the new account information. Employees should be asked to review the list to become familiar with the names, places of employment, and occupations of new customers. New business transactions should be compared to those of similar established businesses as part of the review process. ➤

Sharing a list of new customers with employees will often reveal other internal institution information about a customer. For example, the September 11 terrorists had multiple accounts at many of the same institutions. They would open accounts in groups of three or four individuals. One individual would be on several joint accounts with different individuals.

Identifying normal Behavior

Now that we've discussed normal behaviors, let's discuss suspicious behaviors. In addition to preventing criminal activity from getting into the system, the purpose of anti-money laundering training is also to find and stop any illegal activity when it has gotten into the system.

This portion of training should include participant input. Discuss some of the following suspicious situations, what makes them suspicious, and how employees should respond. You may want to split the class into small groups and then discuss the results.

■ Front-line customer contact personnel (tellers, new accounts, or lenders).

- Customer asks specific questions about reporting requirements. (Concerned about sharing certain information about identity or business activities.)
- New customer purchases a CD and immediately wants to use the CD as collateral on a loan.

- Two or more customers enter the institution and go to different tellers to do their transactions. (This may be a sign of "smurfing," also known as a form of structuring. A "smurf" is an individual used to make deposits to related accounts or purchase monetary instruments with cash.)

- Customer visits his or her safe deposit box after turning small denominations of currency into larger denominations. (A sign of hiding funds.)

- Customer wants to establish an account that allows several persons access to the account, but has no personal or business connection with individuals. (This was common behavior for the September 11 terrorists.)

- Same address and signatories are used for different entities, but no reason for arrangement.

- Customer cannot provide clear explanation of business purpose or type of activities expected.

- Customer is reluctant to provide identification.

- There are inconsistencies with documents used to verify customer's identification. (For instance, a passport is from a different country than what is listed on account opening documents.)

■ Front-line cash-handling personnel (tellers).

- Customer makes loan payments made with large amounts of cash.

- Business that is exempt from reporting begins to make unusually large deposits with no explanation.

Exhibit 4

High-risk, less-regulated:

- Money transmitters and check cashers
- Casinos and other gambling establishments
- Securities brokers/dealers (more often will get large deposits with already laundered money in the form of cashier's checks, money orders, and traveler's checks)

High-risk, high volume of cash businesses:

- Restaurants
- Nightclubs
- Car washes
- Retail businesses
- Travel agencies

High-risk businesses, big-ticket items:

- Dealerships (automobile, boat, airplane, etc.)
- Real estate agencies
- Sellers of antiques, art, furs, etc.

High-risk, created for the purpose of financing terrorism:

- Charities
- Foundations (funds obtained through donations, publications, etc.)



Although sophisticated systems are designed to catch particular activities of criminals, your employees are the best watchdogs your institution has for noticing changes in customer behavior.

- Deposits consist mostly of negotiable items of less than \$3,000 and the customer has no business reason for receiving money orders, cashier's checks, or traveler checks as a method of payment.
- Customer goes out of his or her way to deposit or withdraw large amounts of cash.
- Customer makes cash deposits just under the reporting requirement of \$10,000.
- Customer has others make frequent cash deposits to his or her account.
- Customer frequently uses your institution's night deposit or automated teller machine to make large cash deposits.
- Deposits are made with money orders where the serial numbers appear to be consecutive.
- Deposits consist of musty smelling money.

- Frequent checks from casinos are deposited. (Customer buys chips with currency and trades the chips in for casino check.)
- Large amounts of currency are frequently deposited without any legitimate business reason. (Bags full of money — a bank in New York was recently fined because it did not report such activity.)

■ Personnel who monitor transaction activity (bookkeepers, operations, or auditors).

- Dormant account with a small balance begins to have frequent daily deposits of either cash or wire transfers and daily withdrawals.
- Customer overpays credit card bills.
- Customer makes large currency withdrawals from a business account not normally associated with cash transactions.
- Frequent or unusual wire transfers are made to and from a foreign student's account.
- The aggregate amount of deposits made to individual's accounts frequently exceeds expected income.
- Deposits consist mainly of cash and wire transfers from overseas countries. (This was normal activity for the September 11 terrorists.)

Reinforce to participants that it is their responsibility to report suspicious activity to management. They should not be concerned with determining whether the behavior is associated with money laundering or terrorist activity. It is management's responsibility to investigate whether the activity warrants filing a report.

In addition, you should address how an employee should respond to a transaction that seems suspicious.

■ Ongoing training tip. Often bank employees are trained to watch for suspicious activity that involves "structuring," which is when large amounts of cash just under the reporting requirements are deposited. However, criminals have learned the ins and outs of the financial system and use that knowledge to legitimize their money. That is why it is important for institutions to take additional measures to stay one step ahead. Although sophisticated systems are designed to catch particular activities of criminals, your employees are the best watchdogs your institution has for noticing changes in customer behavior.

One practical method for learning about any odd or suspicious activity in your organization is to have regular meetings with your staff. Your staff should be encouraged to discuss activity they felt was questionable, but that did not seem to rise to the level of reporting it or filing a SAR. Many times, an employee will see something that seems out of the ordinary, but because it is a single incident

may disregard it. However, if that event were shared, it may prompt other employees to share similar events or strange behaviors about that customer. The combined information may actually require the filing of a SAR. Keep in mind that it is important to include all employees with customer contact in these discussions. Because of privacy issues, employees are usually discouraged from talking about customers, but in the right context it is appropriate.

Lesson E: **Identifying High-Risk Businesses**

Start this part of the training by explaining high-risk accounts.

It is also important to recognize high-risk business situations. You need to be aware that certain types of accounts are at greater risk for money laundering and terrorist funding. Thus, those intending to launder money may become involved with these types of businesses to “wash” their money because of the high volume of cash received by these types of businesses. These high-risk businesses can make illegally obtained money appear legitimate. For instance, if a high-risk business, regardless of exempt status, begins to make unusually large deposits with no explanation, it may be a sign of money laundering.

For discussion, create lists of high-risk businesses on a dry erase board or flip chart (see Exhibit 4). Discuss what makes these types of businesses high risk.

Keep Current and Communicate

A list of common schemes could very well be outdated shortly after its creation. Thus, it is important to develop systems to discover new money laundering schemes, both in your area and throughout the country. Information concerning new or common schemes is available on the Internet at the FinCEN Web site (www.fincen.gov) and others. You should also network with other institutions in your area to talk about issues they may be encountering.

Remember, it is important to have a communication system within your bank to detect activity that may already be affecting your institution. For example, you may want to allow time at a weekly meeting to raise concerns, em-

phasize an open-door policy, and develop procedures for handling strange or escalating situations.

Follow Up

Your AML training requires ongoing attention and maintenance at all levels. Employees who understand money laundering and have the tools to prevent it are the most important resource in your institution.

After you have provided the initial training, communication and maintenance are essential. Be sure to follow up with ongoing training sessions, especially for new employees. ❖

Have a question or comment? Use the postage-paid reply card provided in this issue or leave a message at (202) 663-5075.

about the authors

Betsy Fredrickson is an attorney in the Legal and Compliance Services area at Bankers Systems, Inc. Fredrickson's focus is on privacy and anti-money laundering laws and she is a key developer of the company's IDFlag™ product, as well as many of the company's other privacy and anti-money laundering solutions. Fredrickson holds a Bachelor's degree in English from the College of Saint Benedict and a Juris Doctorate from the Hamline School of Law.

Shannon L. Bennett is a compliance analyst in the Legal and Compliance Services area at Bankers Systems, Inc. As a compliance professional for Bankers Systems, Bennett is a writer and editor for the company's Bankers Edge™ online training products. Prior to joining Bankers Systems in 1999, she worked for many years as a banker and gained considerable experience developing and conducting training sessions for bank employees. Bennett holds a Bachelor's degree in English and Speech Communication from St. Cloud State University.

The authors can be reached at (800) 397-2341.