

**THE FORENSIC ACCOUNTANT'S ROLE  
(AND MANAGEMENT'S  
RESPONSIBILITIES) IN DETECTING  
MONEY LAUNDERING ACTIVITIES**

**SOMETHING OLD AND SOMETHING NEW**



Presented by **Arthur A. Hayes, Jr.**

**SIXTEENTH  
INTERNATIONAL CONFERENCE**

**April 8 - 12, 2002**

**SCHOOL OF ACCOUNTING  
FLORIDA INTERNATIONAL UNIVERSITY**

# BIOGRAPHICAL FACT SHEET



## **ARTHUR A. HAYES, JR.**

BS, JD, MBA, CPA, CFE, CGFM, DABFE, DABFA

Art Hayes is the Director of the Division of State Audit in the Tennessee Comptroller's Office. He is responsible for the audit of Tennessee's Comprehensive Annual Financial Report (CAFR) and the preparation of the state's Single Audit. As a matter of interest, Tennessee was the first state to be awarded the Government Finance Officers Association's Certificate for Excellence in Financial Reporting for the state's Comprehensive Annual Financial Report.

Mr. Hayes is a past member of the Executive Board of the Government Finance Officers Association (GFOA). He also

- serves *ex officio* on GFOA's Committee on Accounting, Auditing and Financial Reporting (CAAFR), having previously served as the vice chair,
- has served as the chairman of the CAAFR's Auditing Task Force,
- graduated in 1987 from GFOA's Advanced Government Finance Institute,
- has served on the review panel for GFOA's Awards for Excellence Program, and
- contributed to GFOA's *An Elected Official's Guide to Internal Controls and Fraud Prevention*.

He represents Tennessee's Comptroller, John G. Morgan, on the Executive Committees of the National State Auditors Association and the Southeastern Intergovernmental Audit Forum. He has served as chair of the Association's Committee on Joint Audits and Auditing Standards Committee and has been a member of the following committees: Peer Review, Emerging Issues, Training, and Single Audit. As an active member of the Forum, he has

- served as a member of the Forum's program committee and chairman of its training committee,
- served as chairman of the Forum's State and Local Auditors,
- represented the Forum on the President's Council on Integrity and Efficiency.

As a member of the Association of Government Accountants, Mr. Hayes has served on the Association's Awards Committee and has been chairman of the

Financial Management Standards Committee. He has served on the Nashville Chapter's Executive Committee and has been chapter program chairman.

Art received a Bachelor of Science degree with honors from the University of Tennessee. His major was psychology. He obtained his MBA from Tennessee State University and his Doctor of Jurisprudence from the University of Tennessee. Art received both a Dipolmat American Board Forensic Examiners (DABFE) and Diplomat American Board of Forencis Accounting (DABFA) from the American College of Forensic Examiners.

Mr. Hayes is a frequent lecturer, instructor, and speaker at conferences sponsored by

- The American Institute of Certified Public Accountants,
- The Association of Government Accountants,
- The Government Finance Officers Association,
- The Intergovernmental Audit Forum,
- The National State Auditors Association,
- The National Association of State Auditors, Comptrollers, and Treasurers, and
- Many state societies and federal, state, and local agencies.

Mr. Hayes is a native of Nashville, Tennessee. He served in the United States Army in Military Intelligence as a Counterintelligence Agent and a Polish linguist. He is also an eagle scout. Art married the former Kathy Bruce in 1969. They have two daughters, Heather, born in 1978, and Kristin, born in 1981. Heather recently graduated, Summa Cum Laude with special honors as the outstanding Senior in the class of 2001 in the Psychology Department, from The University of Tennessee-Knoxville and will be attending graduate school at Virginia Tech. in the fall of 2001. Her major is Occupational/Industrial Psychology. She will be entering a program in which she will receive both a Masters and a Ph.D. Kristin has just completed her second year at Tennessee Tech. University in Cookeville, Tennessee. Kristin is a Music Performance Major in Flute.

# THE FORENSIC ACCOUNTANT'S ROLE (AND MANAGEMENT'S RESPONSIBILITIES) IN DETECTING MONEY LAUNDERING ACTIVITIES

## SOMETHING OLD AND SOMETHING NEW

*Presented by Art Hayes*

### I. SOMETHING NEW

#### MONEY LAUNDERING

##### A. What is it?

The processing of criminal proceeds to disguise their illegal origin.

When a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or the persons involved in the illegal activity.

Criminals do this by:

1. Disguising the source of the funds;
2. Changing the form of the funds; or
3. Moving the funds to a place where they are less likely to attract attention.

##### B. How is money laundered?

###### 1. Placement

The initial phase

The launderer introduces the illegal profits into the financial system by:

- a. Breaking up large amounts of cash into less conspicuous small amounts, which are then deposited directly into a bank account;
- b. By purchasing a series of monetary instruments which are then collected and deposited into accounts at other locations.

## 2. Layering

After the funds have entered the financial system, the launderer engages in a series of conversions or movements of the funds to distance them from their source by:

- a. Channeling the funds through the purchase and sale of investment instruments;
- b. Simply wiring the funds through a series of accounts at various banks across the world;
- c. Disguising the transfers as payments for goods or services, giving them a legitimate appearance.

## 3. Integration

After the funds have been layered, the launderer then re-enters them into the legitimate economy through investments in:

- a. Real estate
- b. Luxury assets
- c. Business ventures

## C. What are some of its essential traits?

### 1. Strengths:

- a. International in terms of geography;
- b. Varying degrees of sophistication between nations and banking systems;
- c. Varying degrees of concern/laws;
- d. Varying degrees of cooperation and communication between affected parties;
- e. Lots of money for bribes;
- f. Large volume of transactions.

### 2. Weaknesses

#### a. International

The money has to pass through many hands and countries.

There is much more awareness of the problem and a greater commitment by governments to confront it.

Attention is not exclusively on the underlying criminal activities such as drug trafficking.

The negative consequences of money laundering to governments are being recognized, it is not just another white-collar crime.

Lots of opportunities to lose control/make mistakes

- b. The money has to go through banking systems with controls and trails.
- c. The money has to pass through many legal hoops.
- d. The affected parties can communicate-it is hard to out-run them.
- e. You may try to bribe the wrong person or a bribed official may turn.
- f. The transactions leave some kind of trace and they have to look “normal” when they are not.

## **II. THE LEGAL FRAMEWORK—REQUIREMENTS FOR INDIVIDUALS AND INSTITUTIONS**

- A. Registration.
- B. Record-keeping.
- C. Reporting.
- D. Control obligations.
- E. Safe-harbor provisions.

## **III. THE ACCOUNTANT’S PROFESSIONAL RESPONSIBILITIES**

- To detect
  - To report
  - To prevent
- 
- A. As employees of covered institutions
  - B. As consultants to entities
  - C. As internal auditors
  - D. As tax practitioners
  - E. As attestors of affected companies
  - F. As attestors of money launderers
  - G. Duty with regard to illegal acts by clients

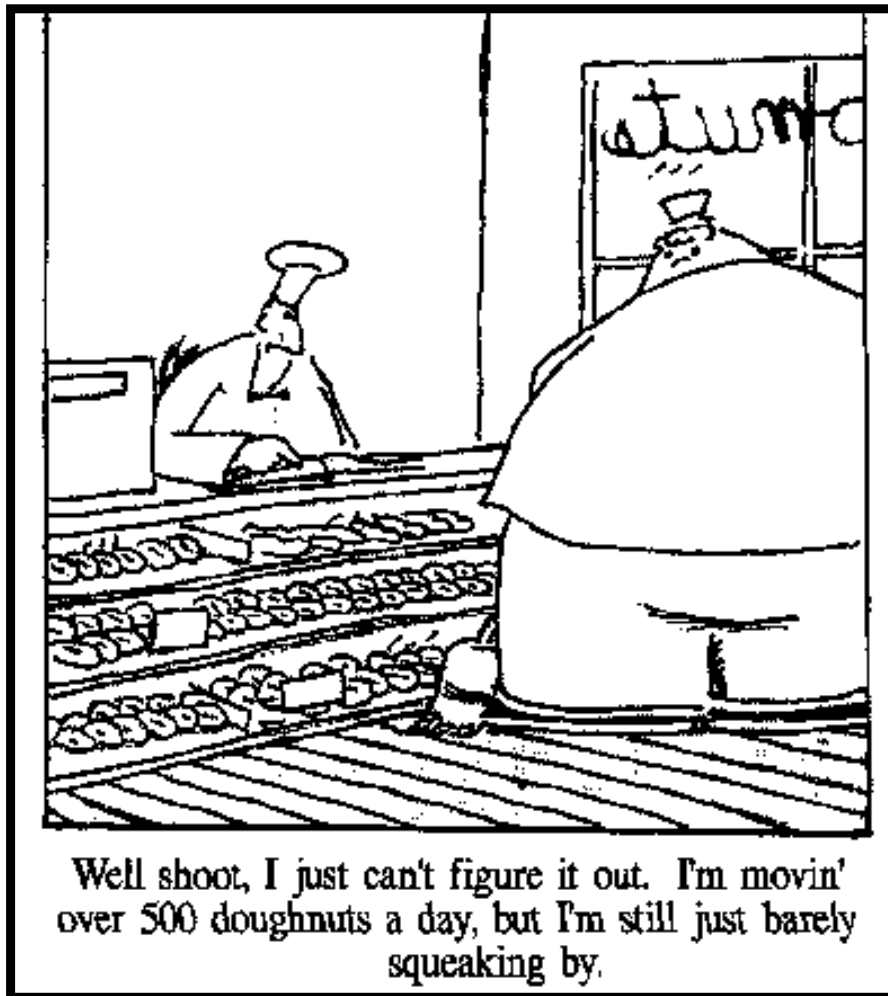
Be aware of the possibility

If specific information comes to their attention must apply specific auditing procedures

H. Securities and Exchange Commission

I. Contingent liabilities

#### IV. SUSPICIOUS ACTIVITIES (BAD SIGNS)



A. In General:

1. Insider abuse involving any amount of funds:
  - Criminal violation(s),
  - Committed or attempted against the financial institution, or
  - Involving financial transactions conducted through the financial institution;
  - Including where the institution was used to facilitate a criminal transaction.
  - The insider was a party in the crime/attempt or aided in the transaction in question.
2. Bribery/gratuities.
3. Check fraud.
4. Check-kiting.
5. Counterfeit activities.
6. False statements.
7. Self-dealing.
8. Misuse of position.
9. Mysterious disappearance.
10. Failure of the financial institution to file currency transaction reports as required
11. Computer intrusions
  - To gain access to a computer system of the financial institution in order to:
    - a. Remove, steal, procure or otherwise affect funds of the institution or the institution's customers.
    - b. Remove, steal, procure or otherwise affect critical information of the institution, including customer account information, or
    - c. Damage, disable, or otherwise affect critical systems of the institution.

B. Money laundering per se:

1. Transactions
  - A deposit
  - Withdrawal
  - Transfer between accounts
  - Exchange of currency

Loan

Extension of credit

Purchase or sale of:

Stock

Bond

Certificate of deposit

Other monetary instrument

Investment security

Any other:

Payment

Transfer

Delivery

By

Through, or

To

A financial institution

Attempted by, or

At, or

Through

The financial institution

If the financial institution knows, suspects, or has reason to suspect the transaction:

- a. Involves funds derived from illegal activities, or  
Is intended or conducted in order to hide or disguise funds or assets derived from illegal activities;  
As part of a plan to violate or evade any law or regulation, or to avoid any transaction-reporting requirement under law.
- b. Is designed to evade any regulations promulgated under the Bank Secrecy Act, or
- c. Has no business or apparent lawful purpose, or  
Is not the sort in which the particular customer would normally be expected to engage, and

The financial institution knows of no reasonable explanation for the transaction after examining the available facts;

Including the background and possible purpose of the transaction

2. Some specific indicators or red flags:

- A request to establish a relationship with, or route a transaction through, a financial institution that is unaccustomed to doing business with foreign persons and that has not sought out business of that type;
- A request to associate any form of secrecy with a transaction, such as booking the transaction in the name of another person or a business entity whose beneficial owner is not disclosed or readily apparent;
- The routing of transactions into or through a secrecy jurisdiction or through jurisdictions or financial institutions that have inadequate customer identification practices and/or allow third parties to carry out transactions on behalf of others without identifying themselves to the institution;
- The routing of transactions through several jurisdictions and/or financial institutions prior to or following entry into an institution in the United States without any apparent purpose other than to disguise the nature, source, ownership or control of the funds;
- The use of accounts at a nation's central bank or other government-owned bank, or of government accounts, as the source of funds in a transaction;
- The rapid increase or decrease in the funds or asset value in an account that is not attributable to fluctuations in the market value of investment instruments held in the account;
- Frequent or excessive use of funds transfers or wire transfers either in or out of an account;
- Wire transfers to or for the benefit of an individual or entity where the beneficial owner or originator information is not provided with the wire transfer, when inclusion of such information would be expected;
- Large currency or bearer instrument transactions either in or out of an account;
- The deposit or withdrawal from an account of multiple monetary instruments just below the reporting threshold on or around the same day, particularly if the instruments are sequentially numbered;
- High-value deposits or withdrawals, particularly irregular ones, not commensurate with the type of account or what is known and documented regarding the legitimate wealth or business of an individual or entity;

- A pattern that after deposit or wire transfer is received by an account, the funds are shortly thereafter wired in the same amount to another financial institution, especially if the transfer is to an account at an offshore financial institution or one in a “secrecy jurisdiction;”
- The frequent minimal balance or zeroing out of an account for purposes other than maximizing the value of the funds held in the account (e.g., by placing the funds in an overnight investment and having the funds then return to the account); and
- An inquiry by or on behalf of an individual or entity regarding exceptions to the reporting requirements of the Bank Secrecy Act (e.g., Currency Transaction Reports and Suspicious Activity Reports) or other rules requiring the reporting of suspicious transactions.

## V. SOMETHING OLD

### A. Basic Auditing

The Hayesways Auditing Mantra

Tell Me

Show Me

Convince Me

### B. The Principle of Least Resistance:

Most individuals take the easiest path from Point A to Point B.

Most individuals find the most efficient methods to get things done, particularly routine things.

Most truthful explanations are relatively straightforward and involve relatively few twists and turns.

When someone has taken too much effort to execute a simple transaction, the auditor/manager should ask why and make sure he/she understands the explanation.

When trying to understand a convoluted transaction, the auditor/manager should try to replicate it using role playing.

The perpetrator is having to take the long way rather than the more direct route because the direct route involves internal controls he/she must bypass or circumvent.

The true reason for the longer path is this circumvention, but the perpetrator has to have a cover story to rationalize the inefficiency.

The cover story represents the real exposure of the perpetrator to detection, if the auditor/manager is diligent in performing follow-up of the representations of the perpetrator.

C. Some old concepts retro-fitted for money laundering:

Most fraudulent activities involve attempts to make those actions appear to be legitimate.

However, when the perpetrator is squeezing these actions into the ordinary channels, there are tale-tell signs.

In general, the activities involve moving more through the pipeline than should be going through it and the perpetrator has to meet the challenge of moving  $X + Y$  through a system that is going to notice the extra  $Y$ .

The normal level of activity is  $X$ , but the perpetrator's challenge is to move  $X + Y$  through the system.

When the illegal activities involve the movement of money through legitimate systems, the perpetrator is faced with the dilemma of having to misstate the true volume of the money or the nature of the transaction.

It is similar to the situation in which the perpetrator is trying to move  $X + Y$  number of goods through a system and make it look like it is just  $X$  passing through.

Money laundering, in particular, forces the perpetrator to try to defy the laws of physics in transforming the nature and size of assets, primarily money, as they pass through the system.

But the perpetrator can neither create nor destroy matter—he/she has to find ways to make the asset appear to be different.

Some of the main tools available to the perpetrator are the same ones we have seen as auditors for years, the level of sophistication may be greater, but there are few ways to really disguise such efforts if we know what to look for. Unfortunately, the auditor may be overwhelmed with the concept of looking for laundered money, just because it has such an exotic label and it is frequently seen as an activity conducted by well-financed operators, in foreign countries, with such high stakes that violence cannot be ruled out as a reaction to detection.

Every perpetrator knows that the clearest way to try to pull off a scam is to try to make the underlying transaction as unclear as possible. They want to avoid clarity and sharp definition.

This is especially true with regard to money laundering.

There are two main facts in money laundering schemes which must be dealt with by the perpetrator: the source of the money, and the identity of the individuals engaged in the activities.

After all, the whole reason for engaging in money laundering is to conceal those two issues. The perpetrator is trying to move ill-gotten funds to another location and into another form of asset without detection of the transaction's nature or the identity of the people involved.

One of the first things the perpetrator seeks is to make the source of funds unclear:

1. Under-stating the total size of the transaction:
  - Split invoices
    - Dividing a large transaction into smaller ones to circumvent a bid requirement.
2. Overstating the total size of one side of the transaction.
3. Overstating the transaction padding of expenses through excessive purchases.
4. Stealing time:
  - Temporarily parking funds so they can be moved again.
  - Engaging in transactions at unusual times.
  - Delaying deposits.
5. Hiding something in plain view:
  - Large movement of funds—payments—from a murky source—from an entity abroad.
6. Failing basic arithmetic.
  - (What a deal! or Man, I was screwed!)
  - The amount of money spent on the items is either far too much or far too little.
7. Buying something not needed, especially services not involving any clear deliverables.
8. The additional issue in money laundering is that the items purchased may be money.
9. Cutting in another player for no apparent business reason (the old straw man conveyance).

Conflicts of interest, the perpetrator creates a company which is not regulated by the money laundering statutes to move the money in and out.

10. Engaging in a totally novel transaction or type of transaction.

## **VI. THE PRIMARY ACTIVITIES OF THE AUDITOR WITH REGARD TO DEVELOPING EVIDENCE**

1. What is normal?
2. What is abnormal?
3. What makes sense?
4. Why did they do it this way?

So how do you find these things?

Know your client.

Ask your client to explain.

## **VII. IDENTIFYING THE TRANSACTIONS**

You are probably going to need a computer

## **VIII. THE PERSPECTIVES**

Your client as the possible perpetrator

The financial conduit for the money laundering

A facilitator for the laundering

A legitimate business front

As an auditor

As a regulator

As a manager

## **IX. UNDERSTANDING THE INTERNAL CONTROLS**

Looking for deviations from their statements/representations.

Those exceptional transactions hidden in the words “usually” “mostly.”

You have to know what is normal/usual.

The kinds of transactions the individual/company engages in.

What is the exchange?

What are they getting for what they are paying?

What do they need the thing for/what do they do with it?

The cycles/timing of those transactions.

Do they correspond with their other business transactions?

The parties involved in those transactions.

Does the institution understand its responsibilities with regard to due diligence?

How aware is the institution, its employees and officers to the problem?

Do they maintain adequate records relating to customer identities?

Are they sufficiently detailed?

Do they take into account any underlying criminal activities?

Are they sensitive to the possibility of shell entities?

Do they retain records for the proper amount of time?

Does the institution have a compliance officer?

What is her background, credentials?

How long has she been in this position?

What did she do before?

What are her priorities?

How do you know?

Any reports?

Any referrals?

Does the institution have a hotline?

Does the institution effectively screen employees?

Background checks?

Credit?

Do they have an internal auditing function?

Does it have money laundering as one of its priorities?

How do you know?

Any on-going training related to money laundering?

By whom?

How often?

How many hours?

Is it effective?

Is the institution attempting to stay abreast of new technologies which can facilitate money laundering and detect it?

Do they invest adequate money and time in these efforts?

Are there audit reports or other reports on the institution revealing either compliance or non-compliance and internal control weaknesses which may relate to the institution's ability to detect and prevent money laundering activities?

Has the institution considered the threat posed by terrorism and the identities of its customers?

Does the institution maintain a proactive stance, including involvement of legal staff, and staff awareness of legal tools and responsibilities—search and seizure and privacy.

## **X. WHAT ABOUT YOU?**

Are you prepared to assist in identifying property for seizure?

Are you prepared to assist in recovery activities including recovery of fines and penalties?