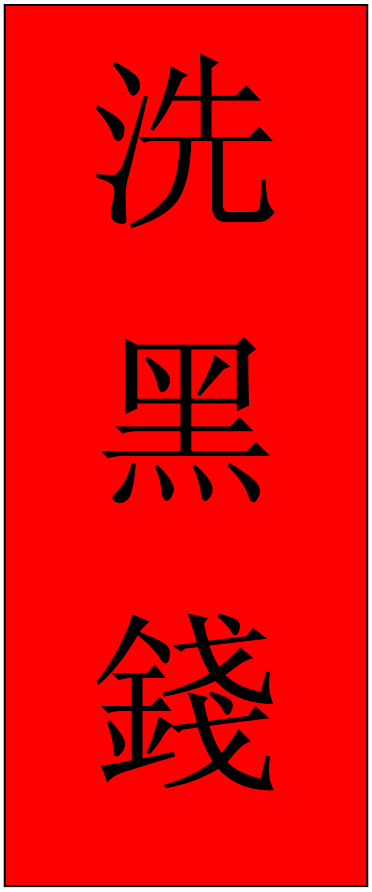
Anti-Money Laundering 101



The Compliance Officers Handbook

Tommy Seah

Anti-Money Laundering 101

Published by CFE-In-Practice

ISBN 981-05-5885-6

LEGAL DEPOSITORY

REPUBLIC OF SINGAPORE

Anti-Money Laundering 101

FOREWORD

In the King James Version of the Bible, Paul wrote to Timothy some two thousands years ago "For the love of money is the root of all evil: which while some coveted after, they have erred from the faith, and pierced themselves through with many sorrows."

1 Timothy 6:10

Today, the world has changed. Men in general not only love money but there are those that devote their lives in laundering money. Money laundering is big business. There is also a great disequilibrium between the risk and the return in Money Laundering activities. This book bores the mark of a man that sets out to neutralize the money launderers' threat to humanity. To appreciate the writings in this book, there is first a need to know the author. Tommy is not your average Joe. He did not do things that most writers do. He did not see the need to leverage on any big accounting firm, Ivy League universities or international associations to do any marketing for his line of services and products. Over the years, without even trying, his name, Tommy Seah, had become the brand name for quality and effective bank product training. This book is the result of his years of training banks in the Asia Pacific region for compliance to Anti-Money laundering regulatory guidelines.

The distinctive feature of this book is that it is written by practitioners for practitioners. As a practicing Certified Fraud Examiner, the author life revolves around solving white collar crimes and international fraud. He has the unfair advantage over the auditors and the big name accountants, in that; he actually works in the field. He has spent no less than twenty eight years of his professional life in neutralizing the threats to financial institutions made by the professional money launderers and white collar criminals.

He also has the benefit of working hands on in many financial organizations in their Anti-Money Laundering programs throughout Asia and the Pacific. The whole point being, in this book, we will tell you, what is money laundering in the real world, how the criminal perpetrate money laundering activities and how they gain penetration into the banks and finally how to prevent and discourage such criminal ambitions and overtures.

Anti–Money Laundering 101

(Anti-Money Laundering - The Compliance Officer's Handbook)

Contents Page

Author's Prologue

A brief history of money laundering

The history of money laundering is, primarily, that of hiding money or assets from the state - either from blatant confiscation or from taxation - and, indeed, from a combination of both. And, of course from those seeking to enforce judgments in civil cases or to follow the money that results from other crime. It is interwoven with the history of trade and of banking.

No one can be really sure when money laundering first began. However, we can be confident that it has been going on for several thousand years. In "Lords of the Rim" Sterling Seagrave explains how, in China, merchants some 2000 years before Christ would hide their wealth from rulers who would simply take it off them and banish them. In addition to hiding it, they would move it and invest it in businesses in remote provinces or even outside China.

In this way, the offshore industry was born, and - depending on your point of view - so was tax evasion. And so were the principles of money laundering - to hide, move and invest wealth to which someone else has a claim.

Over the next four millennia, the principles of money laundering have not changed. But the mechanisms have. Parallel Banking is one of the most durable techniques, or to be more precise suites of techniques.

Over a period of thousands of years, people have used money laundering techniques to move money resulting from crime - but also often to hide and move it out of reach of governments - including oppressive regimes and despotic leaders. Many minorities in countries down the ages and around the world have taken steps to preserve wealth from rulers, both unelected and elected, who have targeted them simply because of their beliefs or color. It is happening even today.

It was several thousand years ago that money and value were separated and value became represented by assets, often assets with no intrinsic worth but increasingly by assets that were recognizable and convertible. So, gold coins were - literally - worth their weight in gold and it was immaterial what country issued them - the only thing that mattered was the quality and quantity of the

gold. Once gold is melted down, it does not lose its value, only its shape. It can be re-fashioned and having arrived in one place as one thing, it can leave there as something else - and that need not even be the same amount of gold. Gold remains one of the main non-currency means of holding money including laundered money. Diamonds are a particular favorite, too. There have been instances of "holy men" carrying laundered funds by concealed diamonds in to California.

Whilst it is true that, in the USA, prohibition and a restriction on gambling made large amounts of cash for those prepared to break the embargoes the most important fact about that time was that it caused a dramatic increase in financial crime - in our definition, financial crime is a crime that gives direct access to the proceeds of the offence. Sanctions busting was a financial crime because for every offence committed, the criminal immediately received cash in his hand. Thus it created an immediate problem over what to do with that money. Opening a cash business was the obvious thing to do. Laundries were a suitable business, and so - goes rumor - the term "money laundering" was invented. This may or may not be true. I think probably not.

Whatever the origins of the term, criminals moved into businesses where the cash crop was higher - including drugs. They formed law firms, accountancy practices, bought banks, film studios, engineering concerns, even governments. At the time of writing this page, one person is trying to buy control of a central bank. If they did not buy the whole organization, they bought - or in some other way obtained the co-operation of - someone within the company. They have always used criminal money to fund the education of the children of the more senior members.

But money laundering also was developed in order to facilitate trade. It is often said (generally without any evidence to support the contention) that Nigeria is the money laundering centre of Africa and that Nigerians around the world are engaged in large scale crime and laundering. Insofar as that is true, the reason for it is because the networks that are now dominated by criminals were set up within the past twenty or so years by international traders who were unable to operate due to exchange control measures and a system of customs inspection that resulted in traders based in Nigeria operating their businesses entirely offshore. Other countries have had - and in the case of some which have strict currency transaction requirements still have - a similar development of

laundering. Money laundering techniques are restricted only by the imagination of the criminals - and there are a lot of criminals trying to find ways to launder.

As businesses worldwide enter the twenty-first century, they face an assortment of risks almost unimaginable just 10 years ago. E-commerce has become ingrained in society with amazing speed: Financial Institutions that cannot keep up are doomed to obsolescence in record time. Technology is driving business models to be retooled in months instead of years. The traditional gatekeepers of information are being supplemented with the Internet democracy in which anyone with a PC can disseminate information widely and quickly—for good or bad. A typical example is financial derivatives, which were originally intended to help manage risk, have themselves created whole new areas of risk for the banks in its anti-money laundering efforts.

It is probably axiomatic that well-managed banks have successful risk management. Over time, a bank that cannot manage its key risks effectively will simply disappear. A simple financial derivatives debacle can decimate staid old institutions over a long weekend. But historically, risk management in even the most successful businesses has tended to be in "silos"—the insurance risk, the technology risk, the financial risk, the environmental risk, all managed independently in separate compartments. **As a strategy, this is fatal.** Coordination of risk management has usually been nonexistent, and the identification of new risks has been sluggish. Money launderers exploit this inherent weakness found in most financial institutions. Office politics and turf issues that create “silos” in financial institutions organizational structure are the money launderer’s favorite playground.

This book looks at a new model—Anti-Money Laundering 101 and enterprise-wide risk management —in which the management of risks is integrated and coordinated across the entire organization. A culture of risk awareness is created.

Notwithstanding uncertainty that abounds in today's economy, farsighted financial institutions have successfully implementing this effective new methodology.

Every organization is, to some extent, in the business of risk management, no matter what its products or services. It is not possible to "create a business that doesn't take risks," according to Richard Boulton and colleagues. "If you try, you will create a business that doesn't make money." As a business continually changes, so do the risks. Stakeholders increasingly want companies to identify and manage their business risks. More specifically, stakeholders want management to meet their earnings goals. Risk management can help them do so. According to Susan Stalnecker, vice president and treasurer of DuPont, **"Risk management is a strategic tool that can increase profitability and smooth earnings volatility."** Senior management must manage the ever-changing risks if they are to create, protect, and enhance shareholder value.

This increasingly risky environment, in which a debacle can have major and far-reaching consequences, requires that senior management adopt a new perspective on risk management. The new perspective should be one that not only prevents debacles but also enhances shareholder value. Indeed, the New Economy calls for a new risk management paradigm that includes Anti-Money Laundering measures as a core component.

This book was first conceived when I was invited to train a European bank in Anti-Money laundering more than six years ago. Since then, I have trained thousands of bankers in Anti-money laundering measures for the purpose of preventing the money launderers from penetrating their respective banks. I have the privilege of training entire bank of different nationalities that stretches as far as Europe to Japan and even the mainland China. One thing came across very clearly. Most bankers are not entirely persuaded that the threat in Money Laundering is real and the training is needful. I found this attitude to be alarming. Most, if not all the participants, perceive the AML training as something that is obligatory because of the mandatory requirements from their respective Central banks.

This is where I believe lies the root of the problem. Most bankers have this very skewed view that being trained in AML about doing the things right for the bank but they do not and have not even begin to understand that their participation to

prevent the money launderers from penetrating the bank is in effect doing the right thing for themselves, their family, their the banks they worked for, and society at large.. I believe most bankers unconsciously believe that anti-money laundering is bad for business. And that is the reason why they have developed this very negative attitude towards the need to be trained in anti-money laundering activities. To compound the problem, most of the books written on this subject tend to be a reproduction of the Financial Action Task Force Guidelines, the European Union legislation for Financial and Economic Crime and or the domestic Central bank guidelines on anti-money laundering. At their very best, it is just able to tell the reader what the subject is all about from the regulators perspective. Very seldom, if at all, is there a book that sees things from the bank or the insurance company's perspective. I tend to suspect that because most of these writers are lawyers, they do not had any real hands-on operational experience in anti-money laundering, they find it easier to regurgitate whatever that has been promulgated by the authorities. It is indeed a case of the half blind leading the blind. This can be very easily confirmed by asking the bank's management a very direct and simple question, "Other than seeking the advice of the external counsels and reading terms and conditions on bank documents, what does your in house legal counsel do?"

This book is written with the end objective of addressing the needs of the bank's compliance officers. So, if you happen to be the legal counsel, I hope you are not one of those that are beyond learning. It will not only tell you what is money laundering but also how to prevent money launderers from targeting and penetrating your bank. Towards the end of the book, you will also find a sample audit program to assist you in determining whether you have discharged your function as a Compliance Officer effectively. This audit program is based heavily on the COSO framework. In 1992, the American Institute of Certified Public Accountants (AICPA), the Institute of Internal Auditors, the American Accounting Association, the Institute of Management Accountants and the Financial

Executives Institute issued a jointly prepared body of work entitled Internal Control – An Integrated Framework.

This authoritative document identifies the fundamental and essential objectives of any business or government entity: economy and efficiency of operations, including safeguarding of assets and achievement of desired outcomes; reliability of financial and management reports; and compliance with laws and regulations. The Internal Control-Integrated Framework, issued by the Committee of Sponsoring Organizations of the Tread way Commission in 1992, (COSO report) has become a widely accepted basis for developing business control systems and assessing their effectiveness. This information tool was developed to help end-users of derivative products establish, assess, and improve internal control systems using the COSO Framework. Many of the control considerations discussed in COSO are also applicable to money laundering.

To achieve quality, processes must first be in control. To improve quality, controlled processes must be measured and evaluated to identify obstacles to success. Effective internal control opens the door that leads to achievement of success. The approach presented by the Framework goes directly to the one key issue of any business – is there reasonable assurance of achieving our mission, objectives, goals and desired outcome, while adhering to laws and regulations; and can we accurately report our success and outcomes to the public and interested third parties.

The COSO framework describes a unified approach for evaluation of the internal control systems that management has designed to provide reasonable assurance of achieving the fundamental anti-money laundering business objectives.

Section ONE

Publicized money laundering scandals.

In recent years, we've seen a growing number of highly publicized money laundering scandals.

They have involved major national and international providers of diversified financial services, along with their correspondents in "off-shore" jurisdictions such as Russia, other former Soviet Republics, Latin America and the Caribbean. Asia is also very much affected by the penetration attempts of the money launderers.

Increasingly, money laundering has also become a problem in many emerging financial services sectors.

In addition, the events of September 11, 2001 and the many subsequent acts of terrorism around the world have prompted a whole new emphasis and "war" on terrorist financing, frequently referred to as "money laundering in reverse" – i.e., money that starts out legitimate and grows "dirty" in its ultimate purpose.

In response, governments and other legal authorities in various jurisdictions have accelerated their issuance of new legislation, regulations, programs and cooperative actions, pronouncements and enforcement steps focused on combating money laundering, terrorist financing and related financial crime. Twenty years after experts first tried to estimate the size of the problem; it is still widely held that money laundering continues to be a US $1 trillion-per-year problem.

In June 2000, the OECD's Financial Action Task Force (FATF), the world's Anti–Money Laundering (AML) watchdog, cited various "non-cooperative" jurisdictions for having serious deficiencies in their AML programs.

This prompted a series of related initiatives:

• The UK, the US and other countries issued parallel money laundering advisories against those same jurisdictions.

• In the autumn of 2000, the international press took up the cause, publishing various articles on money laundering detection and deterrence problems in many "higher-risk" jurisdictions.

• Also in October 2000, in an effort to more clearly identify money laundering and corruption as interrelated problems, a dozen of the world's largest (primarily European and US) banks, working with the anti-corruption arm of the OECD and Transparency International, issued the Wolfsburg AML Guidelines.

• Governments and intergovernmental organizations (IGOs) then issued similar new national and transnational guidance. For example, the US Treasury Department released Guidance on Enhanced Scrutiny for Transactions That May Involve the Proceeds of Foreign Official Corruption.

• Shortly after that, the Basel Committee on Banking Supervision issued its proposal, "Customer Due Diligence for Banks," outlining procedures in four areas: customer acceptance, customer identification, monitoring of high-risk accounts and risk management.

The September 11, 2001 terrorist attacks on the United States and the rapid passage of the USA PATRIOT Act of 2001 began a new global round of tougher AML legislation and related regulatory and law enforcement initiatives that remain very much in motion today.

Below is a summary of significant events in anti-money laundering and combating the financing of terrorism (AML/CFT) field.

1986	United States enacts Money Laundering Control Act, Title 18 U.S. Code, Section 1956 (First Money Laundering Law in the World)
1988	Basel Committee on Banking Supervision – Prevention of criminal use of the banking system for the purpose of Money-Laundering United Nations - Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances ("Vienna Convention")
1989	Financial Action Task Force (FATF) - Established by G-7 in Paris
1990	Financial Action Task Force (FATF) - 40 Recommendations Caribbean Financial Action Task Force (CFATF) - Established Caribbean Financial Action Task Force (CFATF) - 19 Recommendations Council of Europe: Convention on Laundering, Search, Seizure and Confiscation of the Proceeds of Crime (ETS Nº 141) ("Strasbourg Convention")

1991	Financial Action Task Force (FATF) - Mutual Assessment Process Agreed European Union (EU) - Council Directive on prevention of the use of the financial system for the purpose of money laundering (91/308/EEC)
1992	Organization Of The American States / Inter-American Drug Abuse Control Commission (OAS/CICAD) -Model Regulations Concerning Laundering Offenses Connected to Illicit Drug Trafficking Caribbean Financial Action Task Force (CFATF) - Kingston Declaration on Money Laundering
1995	Egmont Group - Established Organization Of The American States / Inter-American Drug Abuse Control Commission (OAS/CICAD) - Summit of the Americas Ministerial Conference Concerning the Laundering of Proceeds and Instrumentalities of Crime - Ministerial Communiqué
1996	Financial Action Task Force (FATF) - 40 Recommendations (First Revision) Financial Action Task Force (FATF) - First Typology Report Issued

1997	Asia / Pacific Group on Money Laundering (APG) - Established Council of Europe (CoE) - Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures (PC-R-EV) - Established Basel Committee on Banking Supervision (BCBS) - Core Principles for Effective Banking Supervision Organization for Cooperation and Economic Development (OECD) - Convention on Combating Bribery of Foreign Public Officials in International Business Transactions
1998	United Nations (UN) - Political Declaration and Action Plan against Money Laundering Adopted at the Twentieth Special Session of the United Nations General Assembly Organization Of The American States / Inter-American Drug Abuse Control Commission (OAS/CICAD) -Model Regulations Concerning Laundering Offenses Connected to Illicit Drug Trafficking and Other Serious Offenses (Amended) International Organization of Securities Commissions (IOSCO) - Resolution on the Adoption of the Objectives and Principles of Securities Regulation United Kingdom (UK) - Regulation of the Financial Services in the Crown Dependencies ("Edwards Report")

1999	United Nations - International Convention for the Suppression of the Financing of Terrorism United Nations (UN) Office on Drugs and Crime - Model Legislation on Laundering, Confiscation and International Co-operation in Relation to the Proceeds of Crime [for civil law jurisdictions] Organization for Cooperation and Economic Development (OECD) - Principles of Corporate Governance Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) - Established United Kingdom (UK) - Review of Financial Regulation in the Caribbean Overseas Territories and Bermuda ("KPMG Report")
2000	Financial Action Task Force (FATF) - Establishes Criteria for Non-Cooperative Countries and Territories (NCCT) List Financial Action Task Force (FATF) - First NCCT List Issued Financial Action Task Force of South America Against Money Laundering (GAFISUD) - Established United Nations (UN) Office on Drugs and Crime - Model Money Laundering and Proceeds of Crime Bill [for common law jurisdictions]

	United Nations (UN) - Convention Against Transnational Organised Crime ("Palermo Convention") International Association of Insurance Supervisors (IAIS) - Insurance Core Principles and Methodology Wolfsberg Group - Private Banking Principles (Original Release - "Wolfsberg Principles")
2001	United Nations (UN) - Security Council Resolution 1373 (2001) [S/RES/1373 (2001)] Basel Committee on Banking Supervision – Customer Due Diligence for Banks International Monetary Fund (IMF) - Public Information Notice (PIN) 01/41 - money laundering poses a threat to financial system integrity, and may undermine the sound functioning of financial systems, good governance, and the fight against corruption. Financial Action Task Force (FATF) - Special Recommendations on Terrorist Financing Financial Action Task Force (FATF) - Behind the Corporate Veil, November 2001 US Government - Guidance on the Proceeds of Foreign Corruption

	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) - Enacted European Union (EU) - Directive (2001/97/EC) of the European Parliament and of the Council of 4 December 2001 amending Council Directive (91/308/EEC) on the prevention of the financial system for the purpose of money laundering
2002	Basel Committee on Banking Supervision - Sharing of Financial Records Between Jurisdictions in Connection With the Fight Against Terrorist Financing Council of Europe (CoE) - Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures - Changes name to (MONEYVAL) (formerly PC-R-EV) European Union (EU) - Final Declaration Against Money Laundering ("Paris Convention") Financial Action Task Force (FATF) - Guidance on Terrorist Financing Financial Action Task Force (FATF) - Guidance on Terrorist Financing, SR VIII: Combating the Abuse of Non-Profit Organisations - International Best Practices International Association of Insurance Supervisors (IAIS) - Anti-Money Laundering Guidance Notes for Insurance Supervisors and Insurance Entities

	International Organization of Securities Commissions (IOSCO) - Objectives and Principles of Securities Regulation (Second Revision) International Monetary Fund (IMF) - Report on the Outcome of the FATF Plenary Meeting and Proposal for the Endorsement of the Methodology for Assessing Compliance with Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) Standard United Nations (UN) - Security Council Resolution 1390 (2002) [S/RES/1390 (2002)] Wolfsberg Group - Private Banking Principles (First Revision) Wolfsberg Group - Correspondent Banking Principles Wolfsberg Group - Statement on the Suppression of the Financing of Terrorism ("Wolfsberg Statement")
2003	Basel - General Guide to Account Opening and Customer Identification (Attachment to Customer Due Diligence Paper) Financial Action Task Force (FATF) - 40 Recommendations (Third Revision) Financial Action Task Force (FATF) - Guidance on Terrorist Financing, SR VI (Alternative Remittance) Interpretive Note Financial Action Task Force (FATF) - Guidance on Terrorist Financing, SR VII (Wire Transfers): Interpretive Note

	Financial Action Task Force (FATF) - Guidance on Terrorist Financing, SR VI: Combating the Abuse of Alternative Remittance Systems - International Best Practices International Association of Insurance Supervisors (IAIS) - Insurance Core Principles and Methodology (Second Revision) International Organization of Securities Commissions (IOSCO) - Objectives and Principles of Securities Regulation (Third Revision) United Nations (UN) - Convention Against Corruption United Nations (UN) - Convention Against Illicit Drugs Wolfsberg Group - Statement on Monitoring Screening and Searching
2005	International Association of Insurance Supervisors (IAIS) - Insurance Core Principles on Corporate Governance Organization for Cooperation and Economic Development (OECD) - Principles of Corporate Governance (Second Revision) Financial Action Task Force (FATF) - Guidance on Terrorist Financing, Special Recommendation IX: Cash Couriers Financial Action Task Force for the Middle East-North Africa (MENAFATF) - Established

	Financial Action Task Force Eurasian Group (EAG) - Established Egmont - Revised Statement of Purpose European Union (EU) - 3rd Directive of the European Parliament Proposed
2005	European Union (EU) - Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing on Terrorism (updates 1990 Convention)
2006	CFE-In-Practice published Anti-Money Laundering 101, The Compliance Officers Guide Book for the Financial Industry

Today, after more than 30 years of AML legislation, numerous intergovernmental initiatives and considerable law enforcement activity, including many money laundering prosecutions and arrests, regulators continue to sanction leading global financial institutions for compliance and control weaknesses – for having insufficient safeguards for protecting themselves against money laundering and related financial crime.

There is no doubt that "enhanced due diligence," "enhanced scrutiny" and related guidelines for strengthening and further promulgating "Know Your Customer" (KYC) principles (explained in a later section) and suspicious activity reporting (SAR) are, through coordinated intergovernmental efforts, spreading across the globe in the forms of hard and "soft" law and leading practices.

Meanwhile, however, privacy rights initiatives have also continued to gain momentum. As the former serve to foster transparency and the latter may easily serve to deter it, there is a fundamental disparity between these two important objectives.

The Fraud Examiners profession around the world is increasingly involved in both arenas. It has been asked to play various roles in combating corruption, with a new emphasis on ferreting out and investigating "Politically Exposed Persons" (PEPs), money laundering, fraud and related financial crime. At the same time, the profession is promoting specialize training to combat financial and economic crimes in the financial industry.

Both types of activities are presenting unique challenges – and risks – to the Compliance Officer.

Given these events, developments and trends, the purpose of this book is to:

• explore the role of the Compliance Officer, fraud examiners, external auditors and other practitioners in ongoing public and private sector efforts to safeguard against money laundering;

• promote awareness of important issues and how increasing professional obligations pertaining to money laundering relate to, and interact with, corruption and transparency, privacy and consumer protection, as well as other professional services, duties and risk; and

• provide thought leadership, practical guidance on leading practices and a foundation for developing subsequent professional guidance for the banking and financial institutions.

Why the sudden interest in FEC ?

Until relatively recently, the battle against money laundering and related financial crime was the exclusive domain of law enforcement, and for good reason. Most governments around the world define money laundering and the activities that lead to it, such as drug trafficking, as serious crimes. Approximately 15 years ago, forensic accountants started to contribute their skills to detecting possible money-laundering activity buried in the books and records of victimized financial institutions. Now, governments and businesses increasingly look to Certified Fraud Examiners, not only to aid in their monitoring and detection efforts, but also to establish and strengthen controls and safeguards against money laundering, its perpetrators and their accomplices in organized financial crime. This is the logical outcome. External auditors at their very best can only perform the task as forensic accountants. The basis of this belief lies in the very nature and responsibilities of their profession. That is to say, they will not want to shoot their own foot by trying to perform the role as an Investigative Auditor which effectively means an immediate admission of their own incompetence as an external auditor. Certified Fraud Examiners on the other hand are very often Independent Third Parties with CPA credentials that does not do CPA work. That being the case, Certified Fraud Examiner is the only one that is qualified to audit the auditors. This is something that the external audit firm is fully conscious of but as a matter of survival, it is not something that they would like to start a forum. But the FBI recognizes this anomaly and the CFE is the only professional certification that the FBI recognizes for the Special Agent program.

Notwithstanding this, Governments, inter-governmental organizations and the global business community have asked, or have even gone so far as to require, external auditors to contribute to the battle against money laundering in at least two ways.

First, most governments have enacted, or are in the process of enacting, laws and regulations requiring businesses to detect and report to the legal authorities any suspicious activity pointing to possible money laundering. Typically, business owners, directors and employees are obliged to do the same. Therefore, any accountant or auditor, regardless of role or certification, may be similarly subject to such requirements. Internal auditors who conduct or participate in compliance and operational audits, and accountants who have managerial responsibilities for compliance and operational activities, may be particularly affected.

Second, many AML regimes, following the FATF and G-7 models, are requiring businesses to have compliance monitoring programs and to independently test the control environment and effectiveness of these programs. In some cases, internal auditors perform this independent testing. Less frequently, external auditors are engaged to independently test compliance and to report to management and to regulators directly. A handful of governments have, however, enacted or are considering new laws and regulations that would require businesses to have independent audits of their compliance with local AML regimes. Such requirements have tended to take two forms: either an independent third party performs a compliance assurance engagement and directly reports the results to the business and the regulator, or the business performs a self-assessment and an external auditor provides assurance as to the integrity of the resulting report and its assertions. The nature of the engagement will also consider third parties' requests for reports. Hand in hand with these new requirements, the governments are also encouraging leading practices in this area.

Whether or not national AML regimes impose specific duties on the Compliance Officers, practitioners are, of course, subject to local regulatory body standards and guidelines. Few Compliance Officers have, however, established auditing standards or guidance specifically focused on money laundering.

Primarily, this is because money laundering is far less likely to affect financial statements than are such types of fraud as misappropriations. Consequently, it is unlikely to be detected in a financial statement audit. Nevertheless, money-laundering activities may have indirect effects on an entity's financial statements and, thus, are of concern to external auditors.

Local and IAASB auditing standards governing auditors' responsibilities for detecting and reporting illegal acts and for evaluating the control environment are also germane to money laundering (because, at this point, money laundering is considered an illegal and criminal act in most jurisdictions). The upcoming section on "How Money Laundering Ties to Fraud" will discuss how conditions and control deficiencies that may contribute to frauds going undetected may similarly contribute to money laundering going undetected. As this section will establish, however, money laundering and fraud have more differences than similarities.

Again, while external auditors and reviewers of financial statements are unlikely to encounter signs of possible money laundering, other professional accountants and Certified Fraud Examiners may have greater exposure.

The section "Compliance Officers' Roles, Professional and Ethical Obligations and Risks" identifies how the fraud examiner occupations that will be affected and this book will be of greater relevance to them

Background and Understanding - Money Laundering Defined

Money laundering is the funneling of cash or other funds generated from illegal activities through legitimate financial institutions and businesses to conceal the source of the funds.

Money laundering is a global activity that, like the illegal activities underlying it, seldom respects local, national or international borders. As mentioned previously, current estimates of the size of the global annual "gross money laundering product" range from $500 billion to $1.5 trillion.

Only within the past dozen years or so has the world community begun to recognize the threat money laundering poses to the orderly and open development of international financial systems and world trade.

While the activities and methods of money laundering have become increasingly complex and ingenious, its "operations" tend to consist of three basic stages or processes — placement, layering and integration.

Placement is the process of transferring the proceeds from illegal activities into the financial system in a way that financial institutions and government authorities are not able to detect.

Money launderers pay careful attention to national laws, regulations, governance structures, trends and law enforcement strategies and techniques to keep their proceeds concealed, their methods secret and their identities and professional resources anonymous. Common placement techniques include the structuring of cash payments through legitimate bank and other financial institutions, which may involve deposits or money transfers, or the purchase of money orders, cashiers or travelers' checks or other monetary instruments.

Layering is the process of generating a series or layers of transactions to distance the proceeds from their illegal source and to obscure the audit trail. Common layering techniques include outbound electronic funds transfers, usually directly or subsequently into a “bank secrecy haven” or a jurisdiction with lax record-keeping and reporting requirements, and withdrawals of already placed deposits in the form of highly liquid monetary instruments, such as money orders or travelers checks.

Integration, the final money-laundering stage, is the unnoticed reinsertion of successfully laundered, untraceable funds into an economy. This is accomplished by spending, investing and lending, along with cross-border, legitimate-appearing transactions.

The world's largest and wealthiest economies tend to serve as the primary hosts for money launderers and their operations. These economies generally harbor the greatest demand for illegal drugs, which is still the primary money-laundering activity. Also, to successfully place, layer and integrate their illegal proceeds, the more sophisticated money launderers look for a similarly sophisticated financial services sector.

Emerging financial markets and developing economies are also important targets and easy victims for money launderers, who continually seek out new places and ways to avoid the watchful eye of the law. The consequences of money-laundering operations can be particularly devastating to developing economies. Left unchecked, money launderers can manipulate the host’s financial systems to operate and expand their illicit activities. Apparently legitimate, but criminally owned, businesses financed by laundered capital can quickly undermine the stability and development of established institutions.

Money launderers and their colleagues are often highly intelligent and well-informed criminals, who are able to quickly adapt and change their modus operandi to cope with a growing global profusion of AML laws, regulations and initiatives.

Money laundering is not just about cash and other monetary instruments; neither is it a problem isolated to conventional deposit taking and lending institutions and activities.

Money launderers have greatly diversified their operations across financial services sectors and, increasingly, across the core and non-core financial activities of non-financial services businesses.

PART 2- A BRIEF HISTORY

The term "money laundering" is said to originate from Mafia ownership of Laundromats in the United States. Gangsters there were earning huge sums in cash from extortion, prostitution, gambling and bootleg liquor. They needed to show a legitimate source for these monies. One of the ways in which they were able to do this was by purchasing outwardly legitimate businesses and to mix their illicit earnings with the legitimate earnings they received from these businesses. Laundromats were chosen by these gangsters because they were cash businesses and this was an undoubted advantage to people like Al Capone who purchased them.

Al Capone, however, was prosecuted and convicted in October, 1931 for tax evasion. It was this that he was sent to prison for rather than the predicate crimes which generated his illicit income and as such this tale that the term originated from this time is a myth.

Money laundering is called what it is because that perfectly describes what takes place - illegal, or dirty, money is put through a cycle of transactions, or washed, so that it comes out the other end as legal, or clean, money. In other words, the source of illegally obtained funds is obscured through a succession of transfers and deals in order that those same funds can eventually be made to appear as legitimate income.

It would seem, however, that the conviction of Al Capone for tax evasion may have been the trigger for getting the money laundering business off the ground.

Meyer Lansky (affectionately called ‘the Mob’s Accountant’) was particularly affected by the conviction of Capone for something as obvious as tax evasion. Determined that the same fate would not befall him he set about searching for ways to hide money. Before the year was out he had discovered the benefits of numbered Swiss Bank Accounts. This is where money laundering would seem to have started and according to Lacey Lansky was one of the most influential money launderers ever. The use of the Swiss facilities gave Lansky the means to incorporate one of the first real laundering techniques, the use of the ‘loan-back’ concept, which meant that hitherto illegal money could now be disguised by ‘loans’ provided by compliant foreign banks, which could be declared to the ‘revenue’ if necessary, and a tax-deduction obtained into the bargain.

‘Money laundering’ as an expression is one of fairly recent origin. The original sighting was in newspapers reporting the Watergate scandal in the United States in 1973. The expression first appeared in a judicial or legal context in 1982 in America in the case US v $4,255,625.39 (1982) 551 F Supp.314.

Since then, the term has been widely accepted and is in popular usage throughout the world.

Money laundering as a crime only attracted interest in the 1980s, essentially within a drug trafficking context. It was from an increasing awareness of the huge profits generated from this criminal activity and a concern at the massive drug abuse problem in western society which created the impetus for governments to act against the drug dealers by creating legislation that would deprive them of their illicit gains.

Governments also recognized that criminal organizations, through the huge profits they earned from drugs, could contaminate and corrupt the structures of the state at all levels.

Money laundering is a truly global phenomenon, helped by the International financial community which is a 24 hrs a day business. When one financial centre closes business for the day, another one is opening or open for business.

As a 1993 UN Report noted: The basic characteristics of the laundering of the proceeds of crime, which to a large extent also mark the operations of organized and transnational crime, are its global nature, the flexibility and adaptability of its operations, the use of the latest technological means and professional assistance, the ingenuity of its operators and the vast resources at their disposal.

In addition, a characteristic that should not be overlooked is the constant pursuit of profits and the expansion into new areas of criminal activity.

The international dimension of money laundering was evident in a study of Canadian money laundering police files. They revealed that over 80 per cent of all laundering schemes had an international dimension. More recently, "Operation Green Ice" (1992) showed the essentially transnational nature of modern money laundering.

Operation Green Ice and Operation Dinero

In Operation Green Ice, law enforcement from Italy, Colombia, the United Kingdom, Canada, Spain, Costa Rica, the Cayman Islands, and the United States co-operated together to expose the financial infrastructure of the Cali mafia. During the first phase of Operation Green Ice, over $50 million in cash and property were seized and almost 200 people were arrested world-wide, including seven of Cali's top money managers. In addition, valuable information was obtained when the authorities gained access to financial books and records, as well as computer hard drives and discs containing financial transactions and bank account information. During the second phase of Green Ice, nearly 14, 000 pounds of cocaine, 16 pounds of heroin, almost $16 million in cash were seized, and over 40 people were arrested.

During Operation Dinero--a two-and-a-half year undercover investigation involving the DEA and the IRS, as well as law enforcement and police organizations in Italy, Spain, Canada, and the United Kingdom--we penetrated the drug money laundering networks and followed the money trails that led us to the top echelons of the Cali cocaine organizations. Through this investigation the authorities further established direct links among the criminal organizations of the Italian Mafia and the Colombian cocaine Mafia. This was an historical operation also because it was the first time a law enforcement agency established a private bank--operated by undercover agents--as an investigative tool to gain insight into the seamy netherworld of drug money laundering.

The results of Operation Dinero made it an overwhelming success. Over $52 million and 9 tons of cocaine were seized, and 88 people were arrested world-wide. This was cocaine that did not end up on the streets of USA. This is money that will not be used to further the production and distribution of more illegal drugs. And, these are criminals who will not continue to pursue the deadly cycle of drug-related crime and violence.

But the major result of both Operations Green Ice and Dinero was the message it sent to the drug Mafia's-that the number of safe havens for their drug money is quickly dwindling. Law enforcement agencies will continue to use financial investigations like these two highly successful operations against traffickers and money launderers.

Schemes Involving Possible Money Laundering and Terrorist Financing

Below are a series of real cases selected from published reports. They are provided to reinforce the need for comprehensive, board-approved customer due diligence policies, a BSA compliance program, and sound financial and economic crime suspicious activity monitoring systems. They also highlight the risks banks become subject to in the absence of sound anti-money laundering and financial and economic crime program.

Russian Money Laundering Scandal

This scandal became public during the summer of 1999, with media reports of $7 billion in suspect funds moving from two Russian banks through a U.S. bank to thousands of bank accounts throughout the world. Pleadings from subsequent criminal cases indicate that, during a four-year period from 1995-1999, two Russian banks deposited more than $7 billion in correspondent bank accounts at a New York bank. After successfully gaining entry for these funds into the U.S. banking system, the Russian banks transferred amounts from their New York bank correspondent accounts to commercial accounts at the bank that had been opened for three shell corporations. These three corporations, in turn, transferred the funds to thousands of other bank accounts around the world, using electronic wire transfer software provided by the bank. In the aggregate, from February 1996 through August 1999, the three corporations completed more than 160,000 wire transfers.

In February 2000, guilty pleas were submitted by a bank employee and spouse and the three corporations for conspiracy to commit money laundering, operating an unlawful banking and money transmitting business in the United States, and aiding/ abetting Russian banks in conducting unlawful and unlicensed banking activities in the United States. The defendants admitted their money-laundering scheme was designed, in part, to help Russian individuals/businesses transfer funds in violation of Russian currency controls, custom duties, and taxes. The three corporations agreed to forfeit more than $6 million in their New York bank accounts. In August 2000, a federal court held that the United States had sufficient facts to establish probable cause to seize another $27 million from two New York correspondent accounts belonging to a Russian bank.

Operation Wire Cutter

The U.S. Customs Service, in conjunction with the Drug Enforcement Administration (DEA) and Colombian Departamento Administrativo de Seguridad, arrested 37 people in January 2002 as a result of a two-and-one-half-year undercover investigation of Colombian peso brokers and their money laundering organizations. These people are believed to have laundered money for several Colombian narcotics cartels. The peso brokers contacted undercover Customs agents and directed them to pick-up currency in New York, Miami, Chicago, Los Angeles, and San Juan, Puerto Rico, which had been generated from narcotics transactions. The brokers subsequently directed the undercover agents to wire these proceeds to specified accounts in U.S. financial institutions that were often in the name of Colombian companies or banks that had a correspondent account with a U.S. bank. Laundered monies were subsequently withdrawn from banks in Colombia in Colombian pesos. Investigators seized more than $8 million in cash, 400 kilos of cocaine, 100 kilos of marijuana, 6.5 kilos of heroin, nine firearms, and six vehicles.

Khalil Kharfan Organization

The DEA (New York Division Group) and the U.S. Attorney's Office in the Southern District of New York concluded a long-term investigation targeting the money laundering and narcotics activities of the Khalil Kharfan Organization operating in Colombia, Puerto Rico, Florida, and the New York Tri-State area. To date, the investigation has revealed that this organization laundered in excess of $100 million in narcotics proceeds. The organization was extremely sophisticated and used several types of communication devices to expedite the transfer of funds worldwide. The Colombian cell, which had staff stationed domestically in Puerto Rico, Florida, New York, and New Jersey, and international businesses and banks in Panama, Israel, Switzerland, and Colombia, used "members" to open accounts in the names of fictitious businesses allowing monies to be deposited and then transferred. Approximately $1 million has been seized.

Terrorist Activity - High-Risk Geographic Location

A pattern of cash deposits below the CTR reporting threshold generated a Suspicious Activity Report (SAR) filing by a U.S. institution. Deposits were made daily to the account of a foreign currency exchange totaling $341,421 for approximately a two-and-one-half-month period. During the same period, the business initiated 10 wire transfers totaling $2.7 million to a bank in the United Arab Emirates. When questioned, the business owner reportedly indicated he was in the business of buying/selling foreign currencies in Iran, the Persian Gulf States, and other countries in the Middle East, and his business never generated in excess of $10,000 a day. Currency Transaction Report (CTR) for three years reflected cash deposits totaling $137,470 and withdrawals totaling $29,387. The business owner and the cash-out transactions were conducted by nationals of countries associated with terrorist activity. Another U.S. depository institution filed a SAR on this person for an $80,000 cash deposit, which was deemed unusual for his profession. He also cashed two negotiable instruments at the same depository institution for $68,000 and $16,387 according to CTR filings.

Wire Remittance Company

Both a wire remittance company and a depository institution filed SARs outlining the movement of about $7 million in money orders through the U.S. account of a foreign business. The wire remittance company reported various persons purchasing money orders at the maximum face value of $500 to $1,000 and in sequential order. Purchases were made at multiple locations, primarily in the northeastern United States, and several purchases also were reported in the southeast United States. The money orders were made payable to various persons, negotiated through banks in Lebanon, and later cleared through three U.S. institutions. The foreign business endorsed the money orders. In some instances, the funds were then credited to accounts at other U.S. depository institutions or foreign institutions. SARs filed by the depository institution reported similar purchases of money orders in the northeastern United States

negotiated at the foreign business. Various beneficiaries were identified, all with Middle Eastern names. They received amounts ranging from $5,000 to $11,000. The foreign business identified by the wire remittance company also was identified as a secondary beneficiary. The money orders cleared through a foreign bank's cash letter account at the U.S. depository institution.

Travel Agent

An IRS investigation in Virginia was initiated on the owner of a travel agency for currency structuring charges after analysis of SAR and CTR filings. The suspect operated, in addition to the travel agency, a money transmittal business that was wiring funds to his business interests in Lima, Peru, and Bogota, Colombia. An analysis of subsequent SARs and CTRs, coupled with various investigative techniques, including execution of several search warrants, led to the suspect entering a plea to one count of money laundering. The defendant admitted structuring transactions to avoid a CTR filing. The defendant structured deposits totaling between $2.5 to $5 million and used six business accounts at five financial institutions to facilitate his activities. The defendant consented to the administrative forfeiture of monies seized from his business accounts.

Suspicious Activity Report Leads to Embargo Investigation

An investigation of a possible violation of the International Emergency Economic Powers Act was initiated following a SAR filing by a bank in New York. The SAR stated that an unnamed bank vice president in charge of the funds transfer program manipulated four payments to the Sudan totaling $73,000 in violation of the embargo. The subject allegedly manipulated the bank's internal Office of Foreign Assets Control (OFAC) filtering system by either manually overriding its screening and blocking function or by omitting any reference to Sudan and reprocessing the wire transfers through the same filtering system. The case was turned over to OFAC.

Other 101 Money Laundering Methods

- **Structuring ("smurfing")**: Smurfing is possibly the most commonly used money laundering method. It involves many individuals who deposit cash into bank accounts or buy bank drafts in amounts under $10,000 to avoid the reporting threshold.
- **Bank Complicity**: Bank complicity occurs when a bank employee is involved in facilitating part of the money laundering process. Bank complicity is becoming increasingly difficult for criminals to use following the introduction of “Tipping Off” as an offence.
- **Money Services and Currency Exchanges**: Money services and currency exchanges provide a service that enables individuals to exchange foreign currency that can then be transported out of the country. Money can also be wired to accounts in other countries. Other services offered by these businesses include the sale of money orders, cashiers cheques, and travelers’ cheques.
- **Asset Purchases with Bulk Cash**: Money launderers may purchase high value items such as cars, boats or luxury items such as jewelry and electronics. Money launderers will use these items but will distance themselves by having them registered or purchased in an associate's name.
- **Electronic Funds Transfer**: Also referred to as a telegraphic transfer or wire transfer, this money laundering method consists of sending funds electronically from one city or country to another to avoid the need to physically transport the currency.
- **Postal Money Orders**: The purchase of money orders for cash allows money launderers to send these financial instruments out of the country for deposit into a foreign or offshore account.
- **Credit Cards**: Overpaying credit cards and keeping a high credit balance gives money launderers access to these funds to purchase high value items or to convert the credit balance into cheques.
- **Casinos**: Cash may be taken to a casino to purchase chips which can then be redeemed for a casino cheque.

- **Refining**: This money laundering method involves the exchange of small denomination bills for larger ones and can be carried out by an individual who converts the bills at a number of different banks in order not to raise suspicion. This serves to decrease the bulk of large quantities of cash.
- **Legitimate Business / Co-mingling of Funds**: Criminal groups or individuals may take over or invest in businesses that customarily handle a high cash transaction volume in order to mix the illicit proceeds with those of the legitimate business. Criminals may also purchase businesses that commonly receive cash payments, including restaurants, bars, night clubs, hotels, currency exchange shops, and vending machine companies. They will then insert criminal funds as false revenue mixed with income that would not otherwise be sufficient to sustain a legitimate business.
- **Value Tampering**: Money launderers may look for property owners who agree to sell their property, on paper, at a price below its actual value and then accept the difference of the purchase price "under the table". In this way, the launderer can, for example, purchase a $2 million dollar property for $1 million, while secretly passing the balance to the seller. After holding the property for a period of time, the launderer then sells it for its true value of $2 million.
- **Loan Back**: Using this method, a criminal provides an associate with a sum of illegitimate money and the associate creates the paperwork for a loan or mortgage back to the criminal for the same amount, including all of the necessary documentation. This creates an illusion that the criminal's funds are legitimate. The scheme's legitimacy is further reinforced through regularly scheduled loan payments made by the criminal, and providing another means to transfer money.

"Willful blindness" - A common malady among bankers

"… willful blindness arises where a person who has become aware of the need for some inquiry declines to make the inquiry because he does not wish to know the truth. He would prefer to remain ignorant. The culpability [in willful blindness]… is justified by the accused's fault in deliberately failing to inquire when he knows that there is reason for an inquiry." R. v. Sansregret (1985) 45 CR (3d) 193

Example of willful blindness: A salesperson encounters a customer who wants to buy a consumer good or service with $25,000 cash. The customer produces a gym bag containing $25,000 in $20 and $50 bills. In the vast majority of modern Canadian commerce, this is not a normal business transaction, and this method of payment is highly unusual. Though the salesperson instantly suspects something is out of the ordinary, they chose to ignore their suspicion so as not to jeopardize an easy sale.

This is exactly the same kind of things that happened in the insurance and the banking industry. Famous last word of a money launderer would be … they chose to ignore their suspicion so as not to jeopardize an easy sale.

By ignoring such key money laundering indicators, an individual may have directly participated in an illegal process.

Preventive strategies for small and medium businesses

When dealing with your customers, ask yourself these questions:

- How well do I know this customer?
- Does the transaction make sense considering the customer's profile?
- Do I fully understand the transaction the customer wishes to complete?
- Am I comfortable with this transaction?
- Is this the usual method for conducting this type of business transaction?

If in doubt, there may be a possibility that your customer is using your business to launder money.

Excerpts of money laundering fraud investigation in the U.S.A.

The following examples of money laundering fraud investigations are excerpts from public record documents on file in the court records in the judicial district in which the cases were prosecuted. Criminal Investigation special agents participated in these multi-agency money laundering investigations by conducting the complete financial investigative aspects of the case.

Columbia Woman Sentenced for Embezzling $583,173

On September 27, 2004, in Nashville, TN, Julie Ellen Bauer was sentenced to 51 months in prison, followed by five years supervised release and ordered to pay $391,926 in restitution. On March 9, 2004, Bauer pled guilty to one count of money laundering and two counts of bank fraud. Between October 9, 1998 and April 12, 2000, Bauer embezzled approximately $583,173 from bank accounts belonging to Saturn Corporation and EDS and transferred the funds to bank accounts she fraudulently opened and controlled under false pretenses and representations. During the period December 17, 1998 and June 23, 2000, Bauer conducted several monetary transactions, in excess of $10,000, with embezzled funds which affected interstate commerce. These transactions included purchasing a home for $324,776.34, lavish furniture for the home and two Chevrolet Suburbans.

Former City Housing Official Sentenced to 5 Years in Prison

On Monday, September 27, in Oakland, California former City of Hercules Senior Housing Specialist Darrick Jonathan Chavis was sentenced to five years in prison and ordered to repay $390,494 that he and LaMark Kevin Lassiter stole from the city during 2001 and 2002. Chavis earlier pled guilty to mail fraud and filing a false tax return. Lassiter pled guilty to mail fraud and structuring monetary transactions and was sentenced earlier this month to serve two and one-half years in prison. Lassiter was also ordered to repay the same amount to the city. Chavis and Lassiter admitted that Chavis, as the city housing specialist overseeing the city fund known as the Rehabilitation and Beautification Program, created phony applications for funds that were intended to allow qualified city residents to repair their homes. The phony applications for funds used the names of actual Hercules residents without their permission. Chavis approved the funds and then mailed or hand-delivered checks to Lassiter, who posed as a

licensed contractor. Lassiter paid another person to create invoices for repair work done on Hercules homes when, in fact, no work had been done. Chavis and Lassiter then shared the stolen funds. This was a joint investigation with the FBI.

John Kenneth Coil Sentenced to Federal prison in Multi-Million Dollar Racketeering, Obscenity, Fraud, and Tax Evasion Scheme

On September 17, 2004, in Austin, TX, John Kenneth Coil was sentenced to 63 months in prison, followed by three years supervised release, fined $5,000, and ordered to forfeit an estimated $8.1 million in property to the government after pleading guilty to federal charges in connection with a racketeering, obscenity, fraud, and tax evasion scheme. Coil admitted to using front companies to run his "adult" pornography stores as well as putting some properties into the names of some of his children and in "trusts" for his children without their knowledge. Coil also skimmed monies from the stores and failed to file tax returns or disclose such income for tax purposes on returns he did file. The total loss as a result of his scheme exceeded $4.5 million for the tax years 1981-2003. Seven other co-defendants have also been sentenced on tax related charges receiving sentencing ranging from three years probation to 42 months in prison.

Maximum Prison Term for Fraud

On September 14, 2004, in Sacramento, CA, Sharon Macauley was sentenced to 30 months in prison and ordered to pay restitution of $1,040,768 to victims of her fraud scheme. Macauley pleaded guilty to one count of money laundering and one count of mail fraud on January 27, 2004, for falsely telling potential investors that she would use their funds to purchase expensive horses for which buyers had already been found. Almost none of the money Mccauley received from investors was actually used for this purpose, and most of the money any investor did receive in return for their investment, came from monies from new investors.

Former Business Consultant Sentenced to 37 Months in Money Laundering Conspiracy

On September 14, 2004, in Washington, DC, Morton Okin, former business consultant for CRM Communications, was sentenced to 37 months in prison to be followed by 5 years supervised release. Okin was also ordered to pay

$11,096,210 in restitution. CRM Communications was a New York corporation in the business of providing telecommunications equipment and services. In April 1997, CRM obtained a line of credit from Capital Factors, Inc. which was secured by CRM's accounts receivable reports. The reports were used to determine the amount of funds to advance CRM. According to court documents, in or about February 1998, Okin joined a conspiracy with several other individuals to defraud Capital Factors and launder monies through bank accounts within the District of Columbia and surrounding areas. Okin and his co-conspirators created false invoices, set up sham corporations, and altered CRM's monthly bank statements to make it appear that CRM's business and accounts receivables were increasing. The false financial information were transmitted to Capital Factors to support the advance of funds. As a result of the scheme, Union Planters, which purchased Capital Factors, incurred a loss of approximately $13 million.

In addition to Okin, Calvin C. McCants, the organizer of the conspiracy, was entenced to 9 years in prison in June 2004. A third co-conspiractor, Howard Weinstein, was sentenced in August 2004 to 5 years probation. Both McCants and Weinstein were ordered to pay restitution for their part in the $13 million money laundering conspiracy.

Administrator of Internet Pharmacy Scheme Sentenced

On September 10, 2004, in San Diego, CA, Odette Pidermann, administrator of World Express Rx, an on-line pharmacy, was sentenced to 18 months in prison and ordered to pay a fine of $4,000 and ordered to forfeit $55,000 from four bank accounts. In addition, Pidermann was ordered to cooperate with the IRS in paying back taxes. Pidermann had previously pleaded guilty to conspiring to sell counterfeit pharmaceuticals, mail fraud, and smuggling pharmaceuticals. World Express Rx had a website by which customers could order prescription drugs without having a prior prescription. Over the life of World Express Rx, the scheme grossed just under $7 million. Piddermann did not take a regular salary; however, funds were simply transferred to her bank accounts as needed to pay personal expenses.

Springfield Woman Sentenced to Federal Prison

On September 8, 2004, in Springfield, MA, Paulette Martin, was sentenced to 1 year and 4 months imprisonment to be followed by 3 years of supervised release and ordered to pay $1.2 million in restitution to the victims of her fraud. Martin

was convicted by a trial jury of one count of conspiracy and thirty counts of wire fraud on May 26, 2004. Evidence presented during the four-day trial proved that Martin, a Pentecostal pastor, conspired with her roommate, Renee Smith, to defraud multiple victims by making false representations and fraudulent promises to convince them to wire money to her through Western Union. Eight victims recounted that Martin told them the money was to help a wealthy individual from Trinidad who needed funds in order to gain access to his vast wealth. The victims were promised a handsome return on their investments. The evidence presented at trial showed that the stories and promises were false. The scheme ended in March 2003, when Martin and Smith were arrested. Smith pleaded guilty to similar charges and is scheduled to be sentenced on October 8, 2004.

North Carolina Man Sentenced in Real Estate Scheme

On September 2, 2004, in Greensboro, NC, George Monk was sentenced to 87 months in prison, followed by three years supervised release, fined $200, and ordered to pay $224,368 in restitution after pleading guilty to numerous tax and fraud charges. Monk and others devised a scheme to utilize various mortgage brokers to submit materially false information to mortgage lenders to obtain mortgage loans. Monk recruited individuals to act as purchasers or "straw-buyers," he then deceived them into believing that following the purchase of the real estate in their names, that he would pay all monthly mortgage payments and promptly transfer the parcels of real property out of the straw-buyers' name. Monk failed to pay the monthly mortgage payments allowing the property to go into default and causing the sale of the property at foreclosure.

Defendant Sentenced to 77-Months Prison Term for Bank Fraud and Money Laundering

On August 31, 2004, in Miami, FL, David Forbes, Jr. was sentenced to 77 months in prison, followed by 5 years supervised release, and ordered to pay restitution of $292,068, for Forbes' involvement in a bank fraud and money laundering scheme. From July 1998 until March 2000, Forbes conspired to enrich himself unlawfully by depositing stolen, forged, and counterfeited checks into bank accounts and then arranging for the withdrawal of monies against those checks. Forbes also concealed the unlawful proceeds by moving them through various individual and corporate bank accounts that he and his unnamed co-conspirators controlled.

Accountant Sentenced to 37-Month Prison Term for Mail Fraud and Tax Evasion

On August 23, 2004, in Miami, FL, Thomas Sewell, a certified public accountant, was sentenced to 37 months' in prison, followed by three years supervised release, and was ordered to pay restitution in excess of $7 million to the victims. Sewell previously plead guilty conspiracy to commit mail fraud, and for filing false tax returns. Sewell was charged in connection with his participation in an investment fraud scheme, as a result of which investors lost over $7 million. Sewell associated himself with the scheme by recruiting investors from among his accounting practice clientele. Sewell falsely advised his clients that their investments would be safe and that he was personally monitoring the funds. Significantly, Sewell failed to advise his clients that he was receiving commissions on the investments that he brought in and failed to disclose on his 1997 and 1998 federal income tax returns that he had received additional income of more than $140,000 from his participation in the scheme.

Florida Man Sentenced for Concealing $660,000 in Income from Bankruptcy Court

On August 20, 2004, in Denver, CO, Richard Shelby Palmer was sentenced to 24 months in prison for concealing assets in connection with bankruptcy and for money laundering. Palmer agreed to the criminal forfeiture of $49,200, of which $39,197 will be used to pay restitution to creditors. Palmer was also ordered to pay a fine of $6,000. Palmer was one of the founders of a company known as Native American Sales, Native American Company or Companies, and then Native American Systems, Inc. whose primary business involved the sale of computer equipment to the United States Government. On July 25, 1995 Palmer filed a Chapter 13 bankruptcy petition. As part of the defendant's criminal scheme, he directed the accounting department of Native American Systems, Inc. to pay the vast majority of his sales commissions to one of three companies run by him instead of to him directly. Palmer used the commission money deposited into these businesses' accounts for his own benefit, and failed to disclose the vast majority of the money to the bankruptcy court. Palmer concealed over $660,000 in income from the bankruptcy court. According to the plea agreement Palmer concealed some of the money by purchasing a 1997 Chevy Tahoe and a 1993 Mercedes Benz in the name of one of his corporations. He also used $44,988

from another corporation's bank account to make a down payment on a residence, which he titled in the name of his father.

Individual Sentenced in Connection With Scheme to Defraud Investors

On August 11, 2004, in Savannah, GA, Mark Bowlin was sentenced to 32 months in prison, followed by three years supervised release, and ordered to make full restitution to victims in the amount of $2,720,421. Bowlin had previously entered a guilty plea to conspiracy to commit mail and wire fraud and money laundering. Between January 1998 and February 2000 Bowlin and others devised a scheme to obtain investors in Universal Interiors, a corporation through which Bowlin conducted a drywall installation business. Potential investors were told by Bowlin and others that they would receive up to a 40% return on investments over short periods of time. To persuade potential investors to invest in Universal Interiors, Bowlin and others made false representations concerning Universal Interiors, including falsely representing that Universal Interiors had millions of dollars worth of projects on hold until it obtained additional startup capital from investors and falsely stating that investments in Universal Interiors were used strictly to purchase materials and to pay labor with regard to a new project. In fact, the investors own funds were used to pay interest payments back to the investors to create an illusion of profitability. Investor funds were also used for Bowlin's and others' own use and enjoyment, including the purchase of homes, a boat, cars and other expenses.

PinnFund Figure Gets Prison Term, Told to Repay Investors

On August 2, 2004, in San Diego, CA, two defendants associated with the $300 million PinnFund U.S.A. ponzi scheme were sentenced for their participation. Tommy Larsen, former president of PinnLease, Inc., a PinnFund subsidiary, was sentenced to serve 78 months in prison followed by three years supervised release and ordered to pay $6,689,908 in restitution. Larsen's sentenced followed his guilty plea to mail fraud, wire fraud, money laundering, obstruction of justice, and tax evasion. Also sentenced was Kim A. Larsen, the son of defendant Tommy Larsen. Kim Larsen was sentenced to 21 months in prison, followed by two years supervised release and fined $5,000 for his role in the fraudulent equipment lease scheme. Kim Larsen's sentencing was based on his guilty plea to one count of making a false statement to a federal officer.

Woman Sentenced in Money Laundering and Drug Case

On July 16, 2004, in Milwaukee, WI, Sandra Garza was sentenced to 180 months in federal prison, followed by five years of supervised release. Garza pleaded guilty to charges of conspiracy to distribute cocaine and money laundering. According to the plea agreement, Garza, her fiancé Maurice Shelly, and her sister Nancy Garza were involved in a cocaine trafficking conspiracy from 2000 through 2003 that included distribution in Milwaukee and Chicago. During this time, Sandra Garza purchased residential properties in and around Chicago with an aggregate price of approximately $2 million. The down payments, mortgages, and rehabilitation costs for these properties were paid with proceeds from Garza's cocaine sales. Garza placed several of the properties in the names of other individuals to conceal her ownership, and assisted these individuals in filing false loan applications. Garza agreed to forfeit her interest in these properties and over $400,000 in seized currency, bank accounts, vehicles, and jewelry. Nancy Garza was previously sentenced to 90 months incarceration and Maurice Shelly 196 months.

Defendant Sentenced to 60 Months in Prison

On July 12, 2004, in Denver, CO, Golda Torres-Harvey was sentenced to 60 months in prison and ordered to pay $580,437 restitution to victims of her scheme. According to the indictment, Torres-Harvey devised a scheme to defraud citizens from Mexico who were residing in Colorado, by inducing them through false representation to pay her for assisting them in preparing and submitting applications to the Immigration and Naturalization Service. She charged Mexican immigrants a fee ranging from $1,500 to $2,500 to assist them in filling out INS applications. Also, she instructed the immigrants to obtain money orders payable to "INS" to cover her fees. Torres-Harvey purposefully delayed the filing of applications and mailed the applications without the required fee of $70 or $1,000; she kept the application assistance fees for herself. She opened a bank account in the name of "International Network Service" and had approximately 61 money orders payable to "INS" deposited into that account. Torres-Harvey then closed her business and did nothing to assist her remaining clients and the INS rejected the applications that were mailed with no accompanying fee.

Leader of Multi-Million Dollar Mortgage Fraud Scheme is Sentenced to 64 Months in Prison; Ordered to Pay $2.4 Million in Restitution

On July 8, 2004, St. Louis, MO, Tandy Hairston was sentenced to 64 months in prison and ordered to pay restitution of $2,424,857. According to the facts filed with the court, Hairston owned and operated The Loan Store (TLS) from 1998 to November 2001. TLS operated as a mortgage brokerage service and as a mortgage bank. To operate as a mortgage banker, Hairston applied for and received warehouse lines of credit from several banks. To serve as guarantor on the warehouse lines of credit, he had to show credit-worthiness by submitting accurate personal financial profiles, including personal tax returns. Hairston began to send false financial information to the warehouse line of credit holders to induce them to renew or continue the lines of credit. The false information included false tax returns that had never been filed with the IRS.

Owner of Tulsa Chemical Company Sentenced to Nine Years in Prison

On July 8, 2004, in Tulsa, OK, Steven John Worley was sentenced to 108 months in federal prison, followed by three years of supervised release. Worley pleaded guilty to one count of money laundering conspiracy and one count of conspiracy to possession of list chemicals with intent to distribute. According to the plea agreement, beginning around May 2000, and continuing until May 28, 2003, Worley, a 49% owner in a company known as Allied Chemical Supply, Inc. (ACS), possessed and distributed listed chemicals knowing, intending, or having a reasonable cause to believe that the chemicals would be used to manufacture methamphetamine. Additionally, Worley deposited the proceeds, or directed the proceeds to be deposited into bank accounts under the name ACS from the illegal sales of listed chemicals. Worley also purchased iodine crystals, a substance used in the clandestine manufacture of methamphetamine, with proceeds from prior illegal sales of listed chemicals. According to the information charging Worley, the El Paso Intelligence Center of the Drug Enforcement Administration determined that ACS was statistically the largest known supplier of precursor chemicals used to manufacture methamphetamine in the United States.

Znetix Defendant Sentenced To Four Years In Prison

On July 6, 2004, in Seattle, WA, Kevin McCarthy was sentenced to four years in prison, to be followed by three years of supervised release with restrictive financial and employment conditions. McCarthy pleaded guilty in July, 2002, to

Conspiracy and Mail Fraud and was a key prosecution witness against other Znetix defendants, which resulted in the convictions of those three defendants. As part of his guilty pleas and sentencing, McCarthy also forfeited a residence he had purchased in Bothell, Washington, a home in Arizona, a $5,000 home entertainment center, and the proceeds of bank accounts in Nevis and Nevada.

McCarthy began his employment with Health Maintenance Centers, Inc. (HMC), an affiliate of Znetix, in September, 2000. On April 9, 2001, the State of Washington Department of Financial Institutions, Securities Division, issued a Cease and Desist Order against HMC and Kevin L. Lawrence prohibiting further stock sales. About three weeks after the Cease and Desist Order, Lawrence and McCarthy formed Cascade Pointe LLC, which was touted as an independent venture capital firm but was secretly controlled by Lawrence and McCarthy in violation of the State's order. At Lawrence's direction, McCarthy created a number of shell companies and bank accounts in the Carribean island nation of Nevis for himself and other co-defendants. McCarthy used these Nevis companies to funnel money offshore and, by submitting fraudulent stock subscription agreements and financial statements from the Nevis companies, to make it appear that Cascade Pointe had wealthy backers and substantial lines of credit. Cascade Pointe fraudulently raised over $12 million from investors after the State's order.

The charges against McCarthy arose out of the government's investigation of the offer and sale of over $90 million of securities by Znetix, HMC, Cascade Pointe, and other affiliated entities. The conspiracy's ringleader was Lawrence, who entered guilty pleas in July, 2003, to Securities Fraud, Wire Fraud, and Conspiracy, and is currently serving a 20-year prison term. Over the course of about seven years, Lawrence and his co-defendants, including Beaman, Culp, Kuiken, and five additional defendants who previously entered guilty pleas – Donavon Claflin, Clifford Baird, Steven Reimer, James Wuensche, and Alfonso D. Lacson, Jr. – defrauded thousands of investors out of approximately $91 million through a massive conspiracy involving false representations and failures to disclose truthful and accurate information in connection with the sale of the securities. Two additional defendants, Timothy Moody and Alex Lacson, pleaded guilty to related felony charges.