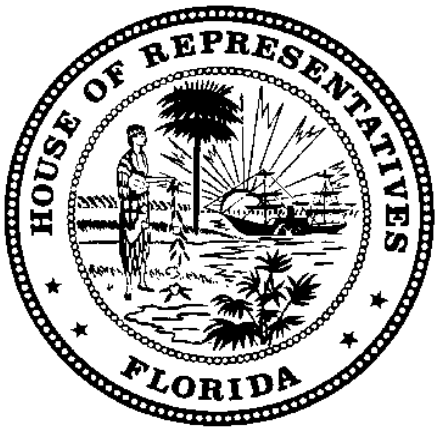
A MONEY LAUNDERING OVERVIEW



Committee on Financial Institutions

Representative Jennifer Carroll
Chair
Representative Garrett Richter
Vice Chair

January 2008

TABLE OF CONTENTS

I. INTRODUCTION

Over the last decade, crimes involving money laundering have risen to astronomical heights. Drug trafficking, alien smuggling, tax evasion, and health care fraud are among the top ranking money laundering offenses plaguing the nation. Consequently, this epidemic has created a problem with multiple facets. As federal and state regulatory agencies, including law enforcement entities collaborate to intensify their focus on money laundering crimes, the State of Florida is also strengthening its efforts.

As an interim project, the Committee on Financial Institutions reviewed Chapter 560, F.S., cited as the Money Transmitters' Code. The project goal of this initial analysis was to assess whether the chapter requires modernization to establish regulatory parallels that correlate with industry innovations and changes in federal regulations, relating to money laundering threats. Staff used a comparative analysis approach to review the national and the Florida money laundering landscapes. This report has two sections.

Since a large amount of comprehensive money laundering research has been conducted from a national perspective, the first section of this report provides an overview of various national money laundering schemes and a summation of tactical efforts being launched at the Federal level. The second section is Florida specific, and it includes a review of the current regulatory endeavors, recommended chapter modernization, and industry innovation.

Various representatives from money services businesses were contacted, and they gave information on industry innovations and regulatory changes. State and national reports cited in the "References" supplied information on money laundering threat assessments including relative federal regulations and policy vulnerabilities. Web sites for the Office of the Comptroller of Currency, (OCC), and the Financial Crimes Enforcement Network, (FinCEN), offered insight into the volume of tainted money circulating through the United States by the globalization of new financial services.

As an introductory closing note, staff extends a special thank you to the Office of Financial Regulation for its assistance.

II. NATIONAL MONEY LAUNDERING OVERVIEW

Background

The world's leading banks have developed an international payment system that helps cultivate global and economic prosperity. The system successfulness is dependent upon speed, accuracy, and geographic reach, but these elements also create vulnerability for instances of money laundering. Considered a very complex crime, money laundering involves intricate details and numerous financial transactions that involve worldwide financial outlets. The Internal Revenue Service defines the term "money laundering" as the activities and financial transactions that are undertaken specifically to hide the true source of the money. In most cases, the money involved is earned from an illegal enterprise and the goal is to give that money the appearance of coming from a legitimate source.

> Once a person is able to inject funds into the payment system that are the product of a criminal act or are intended to finance a criminal act, it is highly difficult, and in many cases impossible, to identify those funds as they move from bank to bank.[1]

According to FinCEN, money laundering involves three different, and sometimes overlapping, stages:

1. Placement involves physically placing illegally obtained money into the financial system or the retail economy. Money is most vulnerable to detection and seizure during placement.

2. Layering involves separating the illegally obtained money from its criminal source by layering it through a series of financial transactions, which makes it difficult to trace the money back to its original source.

3. Integration involves moving the proceeds into a seemingly legitimate form. Integration may include the purchase of automobiles, businesses, real estate, etc.

An important factor connecting the three stages of this process is the "paper trail" generated by financial transactions. Criminals try to avoid leaving this "paper trail" through avoiding reporting and recordkeeping requirements. One way money launderers avoid reporting and recordkeeping requirements is by "structuring" transactions, coercing or bribing employees not to file proper reports or complete required records, or by establishing apparently legitimate "front" businesses to open accounts or establish preferred customer relationships.[2]

In 2005, a group comprised of bureaus and offices within the U.S. Departments of Treasury, Justice, and Homeland Security; the Board of Governors of the Federal Reserve System; and the United States Postal Service studied national money laundering patterns and evaluated the relevant regulations and public policies. The group examined nine money laundering methods, and it issued on January 12, 2006, a report entitled *U.S. Money Laundering Threat Assessment*, (Assessment). "While not exhaustive, the assessment consolidates a tremendous amount of information and insight contributed by the various participating agencies as to the major methods of money laundering that they confront."[3]

On May 3, 2007, the U.S. Departments of the Treasury, Justice, and Homeland Security released the *2007 National Money Laundering Strategy* (2007 Strategy) in direct response to the Assessment. The

---

[1] Guidelines for Counter Money Laundering Policies and Procedures in Correspondent Banking, March 2002, at: http://theclearinghouse.org/000592.pdf

[2] FinCEN: Money Laundering Prevention: A Money Services Business Guide

[3] U.S. Money Laundering Threat Assessment, December 2005, at: http://www.treas.gov/press/releases/reports/js3077_01112005_MLTA.pdf

2007 Strategy identifies areas in which the U.S. government plans to revise, enhance or renew existing federal laws and regulation enforcement; study areas in which new guidance may be appropriate; and work with state supervisory and law enforcement authorities on improving financial transparency within state-regulated financial sectors.

III. FEDERAL STATUTES AND REGULATIONS ENACTED TO ADDRESS MONEY LAUNDERING

There have been several significant pieces of federal legislation enacted to address money laundering. This report takes a glance at two of them.

A. Currency and Foreign Transactions Reporting Act[4]

The "Currency and Foreign Transactions Reporting Act, also known as the Bank Secrecy Act (BSA)[5], and its implementing regulation, 31 CFR 103, are tools the U.S. government uses to fight drug trafficking, money laundering, and other crimes."[6] The BSA is viewed as the nation's first and most comprehensive federal anti-money laundering/counter-terrorist financing statute. Administered by FinCEN, enactment of the BSA primarily is to avert criminal elements from using banks and other financial service providers as conduits to transfer, to deposit, or to hide money derived from illegal activities. These goals may be accomplished by increasing financial system transparency in order to generate paper trails "that law enforcement and intelligence agencies can use to track criminals, their activities, and their assets."[7]

In general, the "reporting and recordkeeping provisions of the BSA apply to banks, savings and loans, credit unions and other depository institutions, and to other businesses defined as financial institutions, including casinos, brokers and dealers in securities, and money services businesses (collectively referred to as "non-banks")."[8]

Several amendments were made to the BSA since its original passage in 1970 that further increased the tools available to law enforcement. Two key provisions are: "The Anti-Drug Abuse Act of 1986, that included the Money Laundering Control Act of 1986 (MLCA), which strengthened the government's ability to fight money laundering by making it a criminal activity. The Money Laundering Suppression Act of 1994 (Title IV of the Riegle-Neal Community Development and Regulatory Improvement Act of 1994) required regulators to develop enhanced examination procedures and increase examiner training to improve the identification of money laundering schemes in financial institutions."[9] National bank compliance with the BSA is monitored by the OCC.

<u>BSA: Money Services Businesses (MSB)</u>

With the exception of a bank or an individual registered with, and regulated or examined by, the Securities Exchange Commission or the Commodity Futures Trading Commission, a MSB is any person or entity, including the United States Postal Service that provides services in one or more of the following capacities:

[4] 31 USC Sections 5311-5330 and 12 USC Sections 1818(s), 1829(b), and 1951-1959.
[5] The BSA is also known as Title 31
[6] Bank Secrecy Act/Anti-Money Laundering: Comptroller's Handbook, September 2000
[7] FinCEN Annual Report 2006
[8] FinCEN: Money Laundering Prevention: A Money Services Business Guide
[9] Id.

Product or Service	Capacity (Type of MSB)-
Money Orders	Issuer of money orders Seller of money orders Redeemer of money orders
Traveler's Checks	Issuer of traveler's checks Seller of traveler's checks Redeemer of traveler's checks
Money Transmission	Money transmitter
Check Cashing	Check casher
Currency Exchange	Currency exchanger
Currency Dealing	Currency dealer
Stored Value	Issuer of stored value Seller of stored value Redeemer of stored value

Source: FinCEN: MSB Services: http://www.msb.gov/msb/index.html (2007)

Notwithstanding the above MSB description, and for purposes of the BSA, entities and persons that conduct MSB-type transactions are not considered MSBs if they do not exchange currency; cash checks; issue, sell, or redeem traveler's checks, money orders, or stored value, in an amount greater than $1,000 to any person on any day in one or more transactions. (See 31 CFR 103.11)

BSA: MSB Requirements

In addition to meeting the MSB BSA requirements for a financial institution, each type of MSB must meet other separate requirements. As summarized from FinCEN data, those additional requirements include:

MSB Registration - Each MSB must register with the U.S. Department of the Treasury, and registration renewal is biennially. Civil fines or criminal prosecution may be imposed for willful violation of the registration requirement. The following list refers to registration exceptions:

- a business that is an MSB solely because it serves as an agent of another MSB;
- a business that is an MSB solely as an issuer, seller, or redeemer of stored value;
- the U.S. Postal Service and agencies of the U.S., of any State, or of any political subdivision of any State.[10]

MSB Agent List - Supplemental to registration, each MSB must prepare and maintain a list of its agents. Agent listings have a five year retention period.

MSB Reporting Requirements – There are twelve separate reports[11] required under the BSA. There is generally a five year retention period for reporting and recordkeeping documents. Concisely, financial institutions submit two to five of the following governmental reports:

1. IRS Form 4789 Currency Transaction Report (CTR): A CTR[12] must be filed for each currency transaction of more than $10,000. Multiple transactions are treated as a single transaction, "if the financial institution has knowledge of: (a) they are conducted by or on behalf of the same person; and (b) they result in cash received or disbursed by the financial institution of more than $10,000. (See 31 CFR 103.22)"[13] In FY 2006, FinCEN reports approximately 16 million Currency Transaction Reports were filed.

[10] FinCEN: Money Laundering Prevention: A Money Services Business Guide

[11] FinCEN Annual Report 2006

[12] The BSA permits banks to exempt certain transactions from the CTR filing requirements.

[13] Bank Secrecy Act/Anti-Money Laundering, Comptroller's Handbook, September 2000.

2. U.S. Customs Form 4790 Report of International Transportation of Currency or Monetary Instruments (CMIR): A CMIR must be filed for individuals or banks that physically, or causes to be physically, transported, mailed, shipped, or received, into or out of the U.S., currency, traveler's checks, and other monetary instruments in an aggregate amount exceeding $10,000. (See 31 CFR 103.23)

3. Department of the Treasury Form 90-22.1 Report of Foreign Bank and Financial Accounts (FBAR): A FBAR must be filed for individuals, including banks, that are subject to U.S. jurisdiction, "having an interest in, signature or other authority over, one or more banks, securities, or other financial accounts in a foreign country, if the aggregate value of any accounts at any point in a calendar year exceeds $10,000."[14] (See 31 CFR 103.24)

4. Treasury Department Form 90-22.47 and OCC Form 8010-9, 8010-1 Suspicious Activity Report (SAR): A SAR must be filed for any perceived suspicious transaction related to unlawful activity. A financial institution must apply due diligence in making its decision about the suspicious nature of a transaction and whether to file a SAR. In FY 2006, FinCEN reports over 1 million SARs were filed. (See 31 CFR 103.18)

5. Designation of Exempt Person Form TDF 90-22.53: A form must be filed to designate an exempt customer for the purpose of CTR reporting under 31 CFR 103.22(d)(3)(i). In addition, banks use this form biennially to renew exemptions for eligible non-listed business and payroll customers. (See 31 CFR 103.22(d)(5)(i)).

MSB – Anti-Money Laundering Compliance (AML) Program – Pursuant "section 352 of the USA PATRIOT Act and implemented by regulation at 31 CFR 103.125"[15] each MSB is required to develop and implement an AML compliance program proportionate with location size, nature of services, and volume of services. Section 352 of the USA PATRIOT Act reads in part:

> SEC. 352. ANTI-MONEY LAUNDERING PROGRAMS.
> (a) IN GENERAL- Section 5318(h) of title 31, United States Code, is amended to read as follows:
>
> (h) ANTI-MONEY LAUNDERING PROGRAMS-
> (1) IN GENERAL- In order to guard against money laundering through financial institutions, each financial institution shall establish anti-money laundering programs, including, at a minimum--
>
> (A) the development of internal policies, procedures, and controls;
> (B) the designation of a compliance officer;
> (C) an ongoing employee training program; and
> (D) an independent audit function to test programs.

MSB - Fund Transfer Rules

As conveyed in FinCEN Advisory - Issue 3: "Funds Transfer: Questions & Answers:"

> The funds transfer rules are designed to help law enforcement agencies detect, investigate and prosecute money laundering and other financial crimes by preserving an information trail about persons sending and receiving funds through funds transfer systems.
>
> Subject to the rules are funds transfers equal to or greater than $3,000 regardless of the payment method.

[14] Bank Secrecy Act/Anti-Money Laundering, Comptroller's Handbook, September 2000.
[15] FinCEN: Money Laundering Prevention: A Money Services Business Guide

MSB - Currency Exchange Record

> If a MSB "provides currency exchanges of more than $1,000 to the same customer in a day, it must keep a record."[16] This record contains information related to single or multiple currencies.

B. USA PATRIOT Act[17]

The official title of the USA PATRIOT Act is "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001." Among its provisions, facilitating the sharing of information between governmental entities and financial institutions forms a pivotal tool in the fight against money laundering and terrorism. The U.S. Department of the Treasury is charged with developing regulations to implement the information-sharing provisions.

Subsection 314(a) of the Act states in part that:

> [t]he Secretary shall . . . adopt regulations to encourage further cooperation among financial institutions, their regulatory authorities, and law enforcement authorities, with the specific purpose of encouraging regulatory authorities and law enforcement authorities to share with financial institutions information regarding individuals, entities, and organizations engaged in or reasonably suspected based on credible evidence of engaging in terrorist acts or money laundering activities.[18]

Subsection 314(b) of the Act states in part that:

> A financial institution or association that transmits, receives, or shares such information for the purposes of identifying and reporting activities shall not be liable to any person under any law or regulation of the United States, any constitution, law, or regulation of any State or political subdivision thereof, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure, or any other person identified in the disclosure, except where such transmission, receipt, or sharing violates this section or regulations promulgated pursuant to this section.[19]

Customer Identification Programs

As a "joint regulation 31 CFR § 103.121 implements section 3261 of the USA PATRIOT Act and requires banks, savings associations, credit unions and certain non-federally regulated banks to have a Customer Identification Program ("CIP")." A CIP is not a stand-alone program, but it comprises an important part of a bank's BSA AML requirements.

Moreover, for a bank to minimally meet the CIP requirements, it must obtain from each customer the following information prior to opening an account: (1) Name; (2) address; (3) date of birth; and (4) an identification number. The program further includes "account-opening procedures that specify the identifying information that will be obtained from each customer and it must include reasonable and practical risk-based procedures for verifying the customer's identity." Such procedures should also "focus on identifying material changes in the agent's risk profile, such as a change in ownership, business, or the regulatory scrutiny to which it is subject."[20]

---

[16] FinCEN: A Quick Reference Guide for Money Services Businesses

[17] 115 STAT. 272 PUBLIC LAW 107–56—OCT. 26, 2001

[18] Federal Register / Vol. 67, No. 187 / Thursday, September 26, 2002 / Rules and Regulations

[19] Id.

[20] Bank Secrecy Act/Anti-Money Laundering Comptroller's Handbook, September 2000

IV. SIGNIFICANT MONEY LAUNDERING SCHEMES

This section only incorporates money laundering schemes that have varying levels of interest and relativity to Florida issues.

Section 1 Banking

Background

Most banks in the United States are commercial banks and serve both the consumer and the business markets. Although bank services vary, banks make application for charter under one of two regulatory designs. Those two charter options make up what is commonly referred to as the dual banking system.

Concisely, the federal design is based on a national bank charter, powers defined under federal law, operation by federal standards, and oversight by a federal supervisor. The state design is characterized by state chartering, bank powers established under state law, and operation under state standards, including oversight by state supervisors.[21]

Banks hold a global fluidity in their ability to operate domestically and abroad. As such, this business group was coined "the first line of defense against money laundering."[22] Through interstate banking, the "dual banking systems remains an important factor underlying the strength and flexibility of our financial system."[23]

Vulnerabilities

Although attempts to launder money through a financial institution can emanate from many different sources, types of entities, and geographic locations, "certain products and services are more vulnerable to money laundering."[24]

a. Identity

An aspect in the difficulty of verifying identification is the growing adoption of the electronic payment systems. Banks and other DFIs[25] face the challenge of reconciling their CIP requirements with customers who attempt to disguise their true identities and sources of income. Technological advances allow for fund transferals via the Internet, for point-of-sale paper check conversion to an electronic debit, and for telephone-initiated payments. These modernized transactions are processed through the automated clearinghouse (ACH)[26]. Consequently, these innovations have created more opportunities for fraud and identity theft. For example, the Assessment cites unauthorized access to checking accounts as one of the fastest growing forms of identity theft.

b. Correspondent Banking

---

[21] Comptroller of the Currency, Administrator of National Banks, National Banks and The Dual Banking System, September 2003

[22] Id.

[23] Remarks by Governor Mark W. Olson, At the Annual Meeting and Conference of the Conference of State Bank Supervisors, Salt Lake City, Utah, May 31, 2002

[24] Bank Secrecy Act/Anti-Money Laundering Comptroller's Handbook, September 2000

[25] The acronym DFI, depository financial institution, encompasses commercial banks, credit unions, savings and loan associations. DFI operations broadly incorporate receiving deposits and providing direct deposit access through payment systems. Other DFI specific transactions are processed through the electronic payment networks are credit and debit cards, bank-to-bank transfers, and paper checks.

[26] The ACH was designed for low value recurring transactions, specifically direct deposit of payroll and monthly consumer bill payments that remain the same each month.

Long in existence and "the heart of the international payment system is correspondent banking"[27] which is a lucrative segment of the banking industry. In sum, correspondent banking involves bank-to-bank financial transactions, such as currency exchanges, wire (funds) transfers, and payable through accounts. By establishing such a relationship, a respondent[28], creates a linkage for its customers to receive many, or all, of the services offered by a U.S. bank, called the correspondent. These accounts introduce direct access to the U.S. financial system, producing the ability to move money within the U.S. and around the world. As a result, correspondent accounts establish "cross-border" relationships conducive to completing transactions without knowing the true payment originator. Moreover, foreign banks[29] can establish "U.S. correspondent accounts with any bank that is authorized to conduct banking activity in the United States, whether or not the foreign bank's parent company is domiciled here."[30]

c. Payable-Through Accounts

Foreign banks may establish with U.S. banks payable-through accounts (PTAs). For a fee, a foreign bank provides to its customers, who are interested in conducting banking in the U.S., access to the U.S. banking system through its PTA(s). Conceivably, these individual and business sub-account holders, which could number in the hundreds, are provided checks by the foreign bank facilitating sub-account holders having the ability to write checks and make deposits directly with the U.S. bank, as if they were the actual account holders.

However, the OCC Handbook stresses PTA activities should not be confused with traditional international correspondent relationships. In a correspondent relationship, a foreign bank enters into an agreement with a U.S. bank to process and complete transactions on behalf of the foreign bank and its customers. Therefore, contractually blocked are those foreign customers having direct access to the U.S. financial system.

d. Offshore or "Shell" Bank

This type of bank typically has no fixed physical presence in the country in which it is licensed, or in any other country, nor is it a branch, or subsidiary, of a bank with a physical presence. There is no physical office where customers go to conduct banking transactions or where regulators go to inspect records and observe banking operations. Secrecy and inaccessibility are the features that lure illicit activity to this entity.

Section 2 Money Services Businesses (MSBs)

Background

> MSBs in the United States are expanding at a rapid rate, often operate without supervision, and transact business with overseas counterparts that are largely unregulated. Moreover, their services are available without the necessity of opening an account. As other financial institutions come under greater scrutiny in their implementation of and compliance with BSA requirements, MSBs have become increasingly attractive to financial criminals.[31]

---

[27] Guidelines for Counter Money Laundering Policies and Procedures in Correspondent Banking, March 2002, at: http://theclearinghouse.org/000592.pdf

[28] A respondent may be a foreign or domestic bank

[29] These banks take the form of: (1) shell banks with no physical presence in any country for conducting business with their clients, (2) offshore banks with licenses limited to transacting business with persons outside the licensing jurisdiction, or (3) banks licensed and regulated by jurisdictions with weak anti-money-laundering controls that invite banking abuses and criminal misconduct.

[30] Correspondent Banking: A Gateway For Money Laundering, By Linda Gustitus, Elise Bean, and Robert Roach, Democratic Staff, Permanent Subcommittee on Investigations, Committee on Governmental Affairs, U.S. Senate, February 2001

[31] U.S. Money Laundering Threat Assessment, December 2005, at: http://www.treas.gov/press/releases/reports/js3077_01112005_MLTA.pdf

Vulnerabilities

This section addresses some of the MSBs identified with vulnerabilities.

a. Issuers/Redeemers/Sellers of Money Order

Federal agencies categorize money orders as a highly versatile vehicle for money laundering. This instrument is "useful for a number of financial crimes ranging from smuggling narcotics, trafficking proceeds, to depositing illicit proceeds from alien smuggling and corporate fraud into bank accounts." Used for varying transactions, an estimated "830 million money orders" are used annually totaling in excess of "$100 billion."[32]

Unlike a traditional customer and banker relationship, money order issuers and sellers lack any rapport with their customers. Minimal, if any, personal information is required to purchase a money order therefore the attractiveness of anonymity lures criminals to this instrument. With nearly complete anonymity, money orders purchased by individuals or groups to mask illegal patterns posture law enforcement in a difficult position. Dollar denominations under $3,000 are available creating an appealing portability, in that the bulkiness of transporting them is minimized compared to cash equivalents. Also, if lost, money orders may be replaced.

U.S. Immigrations and Customs Enforcement, (ICE), Drug Enforcement Administration (DEA), and the regulatory community have reported a steady stream of money order use by launderers moving bulk cash from narcotics transactions. Specifically, ICE and DEA share concern in the Assessment for the increasing numbers of Mexican casas de cambios using money orders to transport illegal proceeds into Mexico. A casas de cambio is a currency exchanger.

b. Money Transmitters

The definition of money transmitter for purposes of BSA regulations includes:

> (i) [a]ny person, whether or not licensed or required to be licensed, who engages as a business in accepting currency, or funds denominated in currency, and transmits the currency or funds, or the value of the currency or funds, by any means through a financial agency or institution, a Federal Reserve Bank or other facility of one or more Federal Reserve Banks, the Board of Governors of the Federal Reserve System, or both, or an electronic funds transfer network; or
>
> (ii) [a]ny other person engaged as a business in the transfer of funds.

Non-bank money transmitters also referred to as money remitter, wire remitter, and wire transmitter. By their "sheer volume and accessibility makes them attractive vehicles to money launderers operating in nearly every part of the world."[33] The inexpensive cash[34] services provided by these entities can be processed instantly or within days thereby creating an opportunity for an initial introduction of illicit proceeds into the payment system. Some money transmitters are registered, but other transmitters are non-registered and operate illegally.

The following list summarizes the nationally recognized vulnerabilities for money transmitters:

a. Structuring transactions that fall below federal reporting limits by using several individuals.
b. Owners or employees of registered transmitters falsifying records that mask large transactions as a sequence of smaller ones, or knowingly providing service to customers with dubious identification.

---

[32] U.S. Money Laundering Threat Assessment, December 2005, at: http://www.treas.gov/press/releases/reports/js3077_01112005_MLTA.pdf

[33] Id.

[34] Certified checks, cashier's checks, money orders, traveler's checks, account withdrawal, credit and debit cards are other sources used to initiate a transfer.

c. Online payment services including acceptance of credit and debit cards, although many financial institutions provide identification safety measures –the lack of face-to-face interaction between the customer and the transmitter may restrict detection of suspicious activity.

Operating under the auspices of retail businesses, such as a grocery store or gas station, a non-registered money transmitter further enhances anonymity. Blanketed by legitimate transactions, non-registered money transmitters generate a "cash-intensive" commerce that legitimizes large deposits and transfers, which possibly veils detection of illicit funds. The following chart plots several observed trends:

Destination	Origin Points	Predominant Predicate Crime
Southern Arizona	California	Narcotics trafficking
Southwest Border	New York, New Jersey, North Carolina, and Florida	Alien trafficking
Texas	New York, Florida, North Carolina, and New Jersey	Alien trafficking and narcotics trafficking-to a lesser extent.

Source: U.S. Money Laundering Threat Assessment, 2005

c. Check Cashers

With some exceptions, a check casher is a person who, for a fee, sells currency in exchange for payment instruments[35]. As an MSB, check cashers are required to register with FinCEN. Although "check cashers are required to file CTRs for cash transactions greater than $10,000, they are not currently required to file SARs (although they may do so voluntarily)."[36]

Third party checking appears to pose the greatest risk exposure. The following scenarios outline the submitted issues confronting law enforcement:

- Money launderers purchasing checks from small businesses with illicit funds. These checks are made out to the business by uninvolved third-party individuals. The business receives the cash equivalent for the checks from a money launderer without incurring any banking charges or income tax reporting, and any bad check instances are passed on to the launderer. The launderer redeems the checks through a check cashing business it controls; he is not personally taking a cash payment (not according to the payee on the checks), and no CTR is filed.
- Money launders sending endorsed third-party checks to accomplices out of the country that are in turn cashed or deposited.

d. Currency Exchangers

The term currency exchanger is interchangeably used with the terms currency dealer, money exchanger, casas de cambio, and bureau de change. This MSB essentially exchanges the currency of one country for that of the same country or for currency of another country, and they use the exchange rates and a commission to gauge their profitability.

This MSB is "subject to the least state regulation, with fewer than ten states[37] currently regulating this activity"[38] However, "certain elements of the currency exchange sector, such as casas de cambios, play a major role in money laundering operations, particularly for narcotics organizations."[39]

Currency exchange businesses may provide a cloak from law enforcement detection by: 1) Exchanging significant quantities of small-denomination bills for large-denomination bills which make bulk shipping

[35] FinCEN: Guidance on Definition of Check Casher and BSA Requirements, January 2003

[36] U.S. Money Laundering Threat Assessment, December 2005, at: http://www.treas.gov/press/releases/reports/js3077_01112005_MLTA.pdf

[37] Florida is a regulatory state.

[38] U.S. Money Laundering Threat Assessment, December 2005, at: http://www.treas.gov/press/releases/reports/js3077_01112005_MLTA.pdf

[39] Id.

easier; and 2) The currency exchanger depositing illicit money into its own commercial account which disguises the origin or source.

Particular attention was made in the Assessment to the casas de cambio. Located primarily along the southwest U.S. border, they specialize in Latin American currencies and transactions. Many casas de cambios offer other services and maybe collocated within other businesses, i.e. gas stations, travel agencies. Cited as generally being non-registered and non-compliant in their filings, "they will commonly move money on behalf of many clients in a bulk transaction conducted under the name of the exchange house, thus cloaking the identity of the true originator."[40] Violations for failure to file CMIRs, CTRs, or SARs point back to the casas de cambios and an "investigative dead end."[41] This scenario also generally describes the Black Peso market in Florida.

e. Stored Value Cards

Stored value cards or pre-paid cards have become a multi-billion dollar industry. It is estimated that consumers nationwide spent nearly $80 billion dollars in 2006 on gift cards alone. Coined as an "alternative for the unbanked and underbanked"[42] stored value cards are outpacing other financial industry products for individuals who lack traditional banking relationships. Hi-tech innovations have broadened the capabilities of this instrument from its embryonic stage as a single or "closed loop" card, used for prepaid telephone calls or retailer-specific purchasing, to a multipurpose, "open loop"[43] financial systems card.

Law enforcement agencies face the vulnerabilities in the below summation:

i. Stored value cards provide a compact, easily transportable and potentially anonymous way to store and access cash value. Also, open system cards lower the barrier to the U.S. payment system, allowing individuals without a bank account to globally access illicit cash via ATMs.

ii. Stored value card programs often accept applications online, via fax, through local check cashing outlets, convenience stores, and other retailers. These programs lack CIPs and systems to monitor transactions for suspicious activity particularly if there are liberal limits or no limits on the amount of cash that can be prepaid into the card account or accessed through ATMs.

iii. Offshore banks also offer stored value cards with international cash access through ATMs. Programs are designed to facilitate cross-border remittance payments that often allow multiple cards to be issued per account.

f. Insurance Companies

The insurance industry has advanced from simply offering its clients life, health, and accident insurance to becoming an investment advising entity that offers diversified portfolios. It is estimated that "more than half a trillion dollars in premiums and contract revenue"[44] are realized by U.S. insurers. Two money laundering targeted areas are term life insurance polices and annuities. Those particular insurance products are available through intermediaries or independent agents; these are individuals who represent several carriers but are not necessarily employed directly by an insurance company. Fortunately, the latitude to probe the background of prospective clients exists, but in some cases, "little know-how or incentive to screen clients or question payment methods exists. In some cases, agents take advantage

[40] U.S. Money Laundering Threat Assessment, December 2005, at: http://www.treas.gov/press/releases/reports/js3077_01112005_MLTA.pdf
[41] Id.
[42] Federal Reserve Bank of New York; Stored Value Cards: An Alternative for the Unbanked, http://www.newyorkfed.org/regional/stored_value_cards.html
[43] The ability to provide global connection for debit and automated teller machine transactions; acceptability wherever Visa or MasterCard are honored. This card type is offered by a wide variety of retail establishments as well as governmental agencies.
[44] U.S. Money Laundering Threat Assessment, December 2005, at: http://www.treas.gov/press/releases/reports/js3077_01112005_MLTA.pdf

of their intermediary status to collude with criminals against insurers to perpetrate fraud or facilitate money laundering."[45]

Strategy Summation

The 2007 Strategy contains nine goals. This report summarizes those tactical efforts that seemingly correlate with issues or interest confronting Florida:

To safeguard the banking system, close collaboration among the FinCEN, the Federal banking regulators, the Federal law enforcement community, and the banking industry: to develop and publish guidance on money laundering threats and application of AML controls; to enhance information sharing and coordinate with law enforcement focused outreach on the value of BSA data; and to aggressively pursue financial crimes.

To disrupt illicit import and export of bulk cash, the U.S. is reviewing the development of a borderless strategy that includes capacity building and cooperation abroad that promotes transparency in the international financial system. The U.S. will provide education, training, and support for countries seeking to protect themselves from money laundering and will work against countries that facilitate money laundering.

The Treasury Department, Office of Foreign Assets Control, IRS, and Federal regulators will enhance awareness of the misuse of legal entities for money laundering by working with state administrators to explore options to increase transparency in ownership, and issue guidance on the risks of providing financial services to shell companies. Federal law enforcement will target for prosecution individuals who use the incorporation process to facilitate money laundering.

Regulatory, supervisory, and law enforcement agencies will coordinate to enforce regulations that extend AML programmatic, reporting, and recordkeeping requirements to the insurance industry.

V. FLORIDA OVERVIEW

This section does not repeat the applicable federal regulations that were discussed in the national overview.

Background

The Office of Financial Regulation (OFR) was created January 7, 2003, to assume oversight regulation of the financial services industries in Florida. This regulatory responsibility was originally held by the Department of Banking and Finance. The mission statement of OFR reads:

> The Office of Financial Regulation (Office) is dedicated to safeguarding the private financial interests of the public by licensing, chartering, examining and regulating depository and non-depository financial institutions and financial service companies in the State of Florida. The Office protects consumers from financial fraud, while preserving the integrity of Florida's markets and financial service industries.

According to OFR, "the regulations under our jurisdiction assist in detecting and deterring money laundering;" however, OFR lacks the authority to investigate "underlying crimes that generated the illicit funds such as drug trafficking." Recordkeeping and reporting requirements help OFR create a "financial

[45] Id.

paper trail that law enforcement and intelligence agencies can use to track criminals, their activities, and their assets."[46]

The examination process is the primary activity of OFR's ability to ensure AML compliance by the entities it regulates. Violation enforcement tools are administrative, and they include powers to issue cease and desist orders; impose administrative fines; suspension, denial or revocation of registration for MSBs, securities dealer, or entity associated persons. Removal of an "individual from working in a state-chartered financial institution" is also within its enforcement purview. (See chapter 655, F.S., Financial Institutions Generally and chapter 896, F.S., Offenses Related to Financial Transactions).

OFR supplied the following data for the number of entities it regulates:

360 Financial Institutions with $107 billion in total assets

3,189 Securities Dealers with over 10,000 branches.

1,543 Money Services Businesses with 2,237 Branches

Funds Transmitters & Payment Instrument Sellers
Firms: 185
Branches: 1,172
Vendors: 37,615

Check Cashers & Foreign Currency Exchangers
Firms: 1,358
Branches: 1, 065

VI. CHAPTER 560, FLORIDA STATUTES, MONEY TRANSMITTERS CODE

A Chapter 560, F.S., Money Transmitters Code

Among its responsibilities, OFR has primary regulatory authority for Chapter 560, F.S., Money Transmitters Code (Code). Enacted in 1994, the Code, among other things, responded at that time to the developing MSB segments. The OFR Bureau of Money Transmitter Regulation is tasked with enforcing the regulatory requirements of the Code.

Modified a number of times over the past 13 years, OFR identify the following dates as most significant:

- 1994 Original Enactment of the Code
- 2000 Incorporated Recommendations of the Money Laundering Task Force
- 2001 Adoption of Part IV (Deferred Presentment)
- 2003 Cabinet Reorganization
- 2004 Enforcement Authority for provisions of USA Patriot Act
- 2006 Electronic Filing and Streamline Renewals

Also, OFR staff considers the 1994 enactment the only comprehensive evaluation of the chapter whereby the industry and effectiveness of the Code was contemplated. The improvements since 1994 create substantial improvements in technology which continue to cut capital and transactional costs within the industry and foster new products and services.

[46] Commissioner Don Saxon, OFR, testimony before the House of Representatives Financial Institutions Committee, Workshop on Money Laundering, December 13, 2007.

The chapter has four parts:

Part I General Provisions (ss. 560.101-560.129):

Section 560.104, F.S., establishes exemptions from the code for the following entities:

> (1) Banks, credit card banks, credit unions, trust companies, associations, offices of an international banking corporation, Edge Act or agreement corporations, or other financial depository institutions organized under the laws of any state or the United States, provided that they do not sell payment instruments through authorized vendors who are not such entities.
>
> (2) The United States or any department, instrumentality, or agency thereof.
>
> (3) This state or any political subdivision of this state.

Part II Payment Instruments and Funds Transmissions (ss. 560.200-560.213), provides in part:

> 560.203 Exemptions.—Authorized vendors of a registrant acting within the scope of authority conferred by the registrant shall be exempt from having to register pursuant to the code but shall otherwise be subject to its provisions.

Sections 560.204-560.205, F.S., provide registration and qualification requirements. Additionally, an initial registration fee not to exceed $500 for each payment instrument seller or funds transmitter and $50 for each authorized vendor or location operating within this state applies.

Section 560.209, F.S., Net worth; corporate surety bond; collateral deposit in lieu of bond reads in part:

> (1) Any person engaging in a registered activity shall have a net worth of at least $100,000 computed according to generally accepted accounting principles. Applicants proposing to conduct registered activities at more than one location shall have an additional net worth of $50,000 per location in this state, as applicable, to a maximum of $500,000.
>
> (2) Before the office may issue a registration, the applicant must provide to the office a corporate surety bond, issued by a bonding company or insurance company authorized to do business in this state.
>
> (a) The corporate surety bond shall be in such amount as may be determined by commission rule, but shall not exceed $250,000. However, the commission and office may consider extraordinary circumstances, such as the registrant's financial condition, the number of locations, and the existing or anticipated volume of outstanding payment instruments or funds transmitted, and requires an additional amount above $250,000, up to $500,000.

Money Transmitters unlike banks cannot accept deposits; however, entities registered under Part II function as money custodians for their customers and are entrusted to fulfill certain financial services

Certain permissible investments are also allowed these entities concisely as follows:

> (1) A registrant shall at all times possess permissible investments with an aggregate market value calculated in accordance with United States generally accepted accounting principles of not less than the aggregate face amount of all outstanding funds transmissions and payment instruments issued or sold by the registrant or an authorized vendor in the United States. (see s. 560.210)

Part III Check Cashing and Foreign Currency Exchange (ss. 560.301-560.310), provides in part:

> 560.303 Requirement of registration.—
>
> (1) No person shall engage in, or in any manner advertise engagement in, the business of cashing payment instruments or the exchanging of foreign currency without first registering under the provisions of this part.
>
> (2) A person registered pursuant to this part may engage in the activities authorized by this part. A person registered under this part is prohibited from engaging directly in the activities that are authorized under a registration issued pursuant to part II, but such person is not prohibited from engaging in an authorized vendor relationship with a person registered under part II.
>
> (3) A person exempt from registration pursuant to this part engaging in the business of cashing payment instruments or the exchanging of foreign currency shall not charge fees in excess of those provided in s. 560.309.

Exemptions to the registration requirements apply to:

> (1) Authorized vendors of any person registered pursuant to the provisions of the code, acting within the scope of authority conferred by the registrant.
>
> (2) Persons engaged in the cashing of payment instruments or the exchanging of foreign currency which is incidental to the retail sale of goods or services whose compensation for cashing payment instruments or exchanging foreign currency at each site does not exceed 5 percent of the total gross income from the retail sale of goods or services by such person during its most recently completed fiscal year.

A registration application requires a nonrefundable fee of $250 for each check casher or foreign currency exchanger and $50 for each authorized vendor or location operating within this state.

Part IV Deferred Presentment (ss. 560.401-560.408) registration requirements are found at s. 560.403, F.S. and reads in part:

> (1) No person, unless otherwise exempt from this chapter, shall engage in a deferred presentment transaction unless the person is registered under the provisions of part II or part III and has on file with the office a declaration of intent to engage in deferred presentment transactions. The declaration of intent shall be under oath and on such form as the commission prescribes by rule. The declaration of intent shall be filed together with a nonrefundable filing fee of $1,000. Any person who is registered under part II or part III on the effective date of this act and intends to engage in deferred presentment transactions shall have 60 days after the effective date of this act to file a declaration of intent.

VI. OTHER FLORIDA STATUTES ENACTED TO ADDRESS MONEY LAUNDERING

A Chapter 655, F.S., Financial Institutions Generally

Chapter 655, F.S., provides general regulatory powers to be exercised by the Financial Services Commission and the OFR in relation to the regulation of financial institutions. OFR has general supervisory powers over all state financial institutions, their subsidiaries, and service corporations, in addition to other powers conferred by the financial institutions codes:

1. Chapter 655, relating to financial institutions generally;

2. Chapter 657, relating to credit unions;
3. Chapter 658, relating to banks and trust companies;
4. Chapter 660, relating to trust business;
5. Chapter 663, relating to international banking corporations;
6. Chapter 665, relating to associations; and
7. Chapter 667, relating to savings banks.

Section 655.031, F.S., provides in part:

> (1) In imposing any administrative remedy or penalty provided for in the financial institutions codes, the office shall take into account the appropriateness of the penalty with respect to the size of the financial resources and good faith of the person charged, the gravity of the violation, the history of previous violations, and such other matters as justice may require.
>
> (2) All administrative proceedings under ss. 655.033 and 655.037 shall be conducted in accordance with chapter 120. . .

The OFR is conveyed authority in s. 655.033, F.S. to issues cease and desist orders, and it is given in s. 655.037, F.S., the ability, for just cause, to issue an order removing a financial institution-affiliated party.

Florida Control of Money Laundering in Financial Institutions Act

Section 655.50, F.S., is known as the "Florida Control of Money Laundering in Financial Institutions Act." The purpose of this section requires submission to OFR of certain reports and the maintenance of certain transaction records involving currency or monetary instruments. These reporting requirements are specifically necessary when such reports and records deter the use of financial institutions to conceal the proceeds of criminal activity and have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings. Many of the section requirements relate to "specified unlawful activity" meaning any racketeering activity as defined in s. 895.02, F.S., such as Chapter 560, relating to money transmitters, if the violation is punishable as a felony. Criminal penalties for a violation of this section range from a first-degree misdemeanor to a first-degree felony, as well as fines and civil penalties.

B Chapter 895, F.S., Offenses Concerning Racketeering and Illegal Debts

Sections 895.01-895.06, F.S., are known as the "Florida RICO (Racketeer Influenced and Corrupt Organization) Act." In s. 895.02, F.S., the term "Racketeering activity" means to commit, to attempt to commit, to conspire to commit, or to solicit, coerce, or intimidate another person to commit any of the offenses specified in the section, such as felonious currency transactions.
Section 895.03, F.S., provides that it is unlawful for any person:

> • who has with criminal intent received any proceeds derived, directly or indirectly, from a pattern of racketeering activity or through the collection of an unlawful debt to use or invest, whether directly or indirectly, any part of such proceeds, or the proceeds derived from the investment or use thereof, in the acquisition of any title to, or any right, interest, or equity in, real property or in the establishment or operation of any enterprise.
>
> • through a pattern of racketeering activity or through the collection of an unlawful debt, to acquire or maintain, directly or indirectly, any interest in or control of any enterprise or real property.
>
> • employed by, or associated with, any enterprise to conduct or participate, directly or indirectly, in such enterprise through a pattern of racketeering activity or the collection of an unlawful debt.
>
> • to conspire or endeavor to violate any of the previously described provisions.

Section 895.04, F.S., provides that a person engaged in activity in violation of s. 895.03, F.S., commits a first-degree felony. In lieu of a fine otherwise authorized by law, any person who derives pecuniary value from a RICO violation or causes personal injury, property damage, or other loss, as a result of such violation, may be sentenced to pay a fine not exceeding three times the gross value gained or three times the gross loss caused, whichever is greater, plus court costs and reasonably incurred investigation and prosecution costs.

Additionally, s. 895.05, F.S., provides civil remedies for RICO Act violations, including forfeiture of property.

C Chapter 16, F.S., Attorney General

Section 16.56, F.S. authorizes the Office of Statewide Prosecution to investigate and prosecute, among other things, any violation of the RICO Act, including any offense listed in the definition of racketeering activity s. 895.02(1)a, under certain circumstances.

D Chapter 896, F.S., Offenses Related to Financial Transactions

Section 896.101, F.S., may be cited as the "Florida Money Laundering Act" This sections prohibits various activities related to proceeds gained from specified unlawful activities. Depending upon the nature and financial amount, criminal penalties range from a third-degree to a first-degree felony.

E Chapter 905, F.S., Grand Jury

Section 905.34 Powers and duties; law applicable, reads in part

—The jurisdiction of a statewide grand jury impaneled under this chapter shall extend throughout the state. The subject matter jurisdiction of the statewide grand jury shall be limited to the offenses of:

> (3) Any violation of the provisions of the Florida RICO (Racketeer Influenced and Corrupt Organization) Act, including any offense listed in the definition of racketeering activity in s. 895.02(1)(a), providing such listed offense is investigated in connection with a violation of s. 895.03 and is charged in a separate count of an information or indictment containing a count charging a violation of s. 895.03, the prosecution of which listed offense may continue independently if the prosecution of the violation of s. 895.03 is terminated for any reason;

VII. RECOMMENDED CHAPTER 560, FLORIDA STATUTES, REVISIONS THAT ADDRESS MONEY LAUNDERING

This section is not a comprehensive money laundering evaluation. However, it speaks to primary issues raised with staff by interested parties regarding needed revisions to Chapter 560, F.S.

Background

According to OFR data, money transmitters pose noteworthy vulnerabilities to criminal entry into the Florida financial system. Currently, it is estimated 37,000 money transmitters operate in Florida. OFR cites the Code changes of 2000 and 2004 as the most relative to money laundering law enforcement. In 2000, the Money Laundering Task Force made improvements to criminal penalties, and in 2004, the OFR Bureau of Money Transmitter Regulation incorporated its initial assessment of the USA PATRIOT Act. However, neither of the changes in 2000 and 2004 made improvements in terms of regulatory authority. It is undisputed that MSBs provide valuable financial services; however, it is critical

that MSBs "maintain the same level of transparency, including the implementation of the full range of anti-money laundering controls required by law, as do banking organizations."[47]

Vulnerabilities

MSBs are required federally to have an AML program; conversely, that requirement does not transcend into a state regulator receiving a MSBs AML program when it makes application for state licensure. According to OFR, a key component to the ultimate success or failure of current enforcement efforts is in the AML arena, for example:

Strategy

MSBs – Generally

Subject to certain limits, require MSBs to incur the cost of OFR examinations,.

Require OFR to examine each MSB at least once every five years.

Require OFR report to the state attorney, appropriate regulatory agency, or other prosecuting agency any alleged criminal violations of law disclosed through its examination or investigation process.

Require OFR to prepare an annual report on actions taken against MSBs and present the report to the Governor, the President of the Senate, and the Speaker of the House of Representatives by July 1.

MSBs (Parts II and III of the Code)

- Make submission of an AML program a condition of licensure. Failure to submit an acceptable plan will be grounds for license denial. (The term "acceptable" will require clarification.)

- Create a state law criminal cause of action for willful violation of federal regulations implementing the BSA.

MSBs (Part II of the Code)

Increase the financial requirements for money transmitters as a method to decrease the likelihood of consumer funds' being lost. For instance:

- Bonding. Require a minimum $50,000 to maximum $2 million bond requirement. The bond requirements will be calculated based on the financial condition, number of locations, and anticipated volume of the licensee. (Clarification as to whether bonding applies to only company-owned locations or company and agent locations will be necessary.)

- Net Worth. Change net worth requirements for each location to $10,000 per location up to a $2 million cap. Revise the calculation of net worth to exclude assets such as goodwill or receivables from officers and other affiliated parties.

- Prohibit a licensee from pledging consumer funds as collateral for its financial obligations or from using consumer funds to operate its business. (Clarification that addresses the implications to s. 560.210, F.S., Permissible investments will be necessary.)

- Authorize OFR to seek restitution for consumers.

[47] FinCEN: April 26, 2005 Advisory: Guidance to Money Services Businesses on Obtaining and Maintaining Banking Services

- Authorize OFR to seek appointment of a receiver in cases other than those cases requiring appointment by a circuit court judge. The duty of the receiver will be to preserve the remaining company assets.

- Require submission to OFR of audited financial statements.

MSBs: Law Enforcement Tools (Part II of the Code)

- Make it a third degree felony to conceal, remove or destroy required records, if done with intent to deceive regulators or law enforcement.

- Make it a third degree felony to knowingly fail to disclose the direct or indirect control of a MSB.

B MSBs: Check Cashers (Part III of the Code)

Similar to schemes observed nationally, OFR has become aware of questionable check cashing practices in three areas:

i) The purchase of checks from other check cashers.

ii) Cashing suspicious corporate checks, and

iii) Cashing third party checks. (The regulatory requirements for cashing commercial checks are currently the same for retail check cashing.)

Strategy

Revise registration criteria for check cashers by eliminating the five percent "incidental business" exemption and adopt the criteria for federal registration that applies to an entity that engages in transactions in excess of $1,000 per person per day.

Prohibit check cashers from accepting multiple checks from any person who is not the original payee unless that person is also a registered check casher.

Require check cashers to deposit or sell all payment instruments accepted within five business days.

Require that all checks accepted by a check casher be endorsed by the payee at the time of acceptance and also be endorsed by any other person attempting to cash the check.

Require check cashers to file SARs with OFR and FinCEN.

Require check cashers to obtain a fingerprint and a photo identification copy from anyone cashing a check in excess of $1,000.

Impose additional reporting, recordkeeping, and regulatory requirements on check cashers who cash third-party or corporate checks exceeding $3,000 to any one person in any one day. The requirements may include:

- Maintaining detailed customer files on corporate entities;
- Maintaining an electronic payment instrument log; and
- Obtaining valid identification from the person receiving the cash.

Industry Innovation

One of the core issues for the check cashing problems is identity validation. In response to this core concern, the Financial Service Centers of Florida shared with staff that certain of its members have

adopted and implemented CIPs of the type applicable to banks, savings associations, and credit unions when opening customer accounts. The below industry innovation shows requirements that could be implemented to minimize fraud relating to customer identification:

When cashing checks payable to companies (CPC), special procedures and applications are developed and used. For all new CPC customers, the customer's company name and address, occupational license number, number of employees, annual payroll, and references are required, as well as the owner's social security number. Other required documentation of CPC customers includes corporate resolutions and affidavits that indicate among other things, the authorization of specific persons to cash checks on behalf of the company, the name and telephone numbers of the company's officers, and the taxpayer identification number. All pages of the applications, resolutions and affidavits must be completed in accordance with the following procedures:

- ✓ All pages must be notarized
- ✓ All pages must include the identification of the customer service representative who notarized the documents;
- ✓ All pages must include the signature and thumb print of the customer;
- ✓ All pages must show the date of completion; and
- ✓ All pages and every section of the application must be completed.

VIII. REFERENCES

Bank Secrecy Act/Anti-Money Laundering: Comptroller's Handbook, September 2000

Comptroller of the Currency, Administrator of National Banks, National Banks and the Dual Banking System, September 2003

Correspondent Banking: A Gateway For Money Laundering, By Linda Gustitus, Elise Bean, and Robert Roach, Democratic Staff, Permanent Subcommittee on Investigations, Committee on Governmental Affairs, U.S. Senate, February 2001

Federal Register / Vol. 67, No. 187 / Thursday, September 26, 2002 / Rules and Regulations

FinCEN: Guidance on Customer Identification Regulation, January 2004

FinCEN: Guidance to Money Services Businesses on Obtaining and Maintaining Banking Services, April 26, 2005

FinCEN: Money Laundering Prevention: A Money Services Business Guide Financial Crimes Enforcement Network U.S. Department of the Treasury Washington, DC

WEBSITES

FDIC Law, Regulations, Related Acts, 8000 - FDIC Miscellaneous Statutes and Regulations, Appendix C to Part 103—Interpretive Rules, Release No. 2004—01,
http://www.fdic.gov/regulations/laws/rules/8000-2060.html

Federal Reserve Bank of New York; Stored Value Cards: An Alternative for the Unbanked
http://www.newyorkfed.org/regional/stored_value_cards.html

FinCEN: A website for money Services Businesses
http://www.msb.gov/msb/index.html

FinCEN: Funds Transfers: Questions & Answers: Date: June 1996 Advisory: Vol. 1, Issue 3
http://www.fincen.gov/advsiii.pdf

Guidelines for Counter Money Laundering Policies and Procedures in Correspondent Banking, March 2002
http://theclearinghouse.org/000592.pdf

Internal Revenue Service: Overview of Money Laundering
http://www.irs.gov/compliance/enforcement/article/0,,id=112999,00.html

National Money Laundering Strategy, 2007
http://www.treas.gov/press/releases/docs/nmls.pdf

U.S. Money Laundering Threat Assessment, December 2005
http://www.treas.gov/press/releases/reports/js3077_01112005_MLTA.pdf

OTHER

Remarks by Governor Mark W. Olson, At the Annual Meeting and Conference of the Conference of State Bank Supervisors, Salt Lake City, Utah, May 31, 2002