RETHINKING PREVENTIVE MEASURES FOR MONEY LAUNDERING AND TERRORISM FINANCING

Richard K Gordon, Case Western Reserve University
RETHINKING PREVENTIVE MEASURES FOR MONEY LAUNDERING AND TERRORISM FINANCING*

RICHARD K. GORDON**

February Draft

INTRODUCTION
I. FAILURES AND SUCCESSES IN PREVENTIVE MEASURES FOR MONEY LAUNDERING AND TERRORISM FINANCING
   A. System Overview
   B. Role of the Private Sector
      1. Customer Identification, Customer Profiling, Record-Keeping
      2. Transaction Monitoring and Suspicious Transaction Reporting
   C. Role of the Public Sector
      1. Overview
      2. Guidelines, Feedback, and Supervision
      3. Suspicious Transaction Analysis and Referral for Investigation
   D. Private Sector Successes and Failures
      1. Overview
      2. Clarity and Objectivity of the Rule
      3. Economic and Regulatory Incentive Effects
      4. Objective Capacity
      5. Issues Unrelated to Effectiveness Implementation
   E. Public Sector Successes and Failures
   F. Summary and Conclusions

II. FAILURES AND SUCCESSES IN SELECTING INCOME TAX RETURNS FOR AUDIT
   A. System Overview
   B. Role of the Private Sector
   C. Role of the Public Sector
   D. Summary and Conclusions

III. PROPOSAL FOR A NEW FRAMEWORK FOR PREVENTIVE MEASURES FOR MONEY LAUNDERING AND TERRORISM FINANCING

CONCLUSION

* © 2010 Richard K. Gordon.
** Associate Professor of Law, Case Western Reserve University School of Law; Adjunct Associate Professor of International Studies, Brown University. B.A. Yale (1978). J.D. Harvard Law School (1984). From 1994 through 2003 the author served as a senior staff member of the International Monetary Fund where he worked, inter alia, on the development and implementation of the international standards for anti-money laundering and terrorism finance. The views expressed in the Article are the author’s alone and should not be attributable to the International Monetary Fund. Thanks to Jonathan Adler, Craig Boise, Emile van de Does de Villebois, Erik Jensen, Rick McDonnel, Dale Nance, Rick Small, and Moni SenGupta.
Preventive measures for money laundering and terrorism financing are among the most widely accepted and observed global standards. However, there is substantial evidence that they do not work well. A main reason is that private sector parties, mostly financial institutions but including few others, are tasked with duties for which they are ill suited, while too little is required of the public sector. While they are required to monitor client transactions and reporting those that raise suspicion of money laundering or terrorism financing, they do not have sufficient expertise or data access to do so. Also, as suggested by the application of theories of private sector compliance with unfunded mandates, there are simply too many disincentives to effective implementation. Dividing these tasks between the private sector and public sector is inherently inefficient; not only does it separate data pools into many different private sector parties and the public sector, it reduces the overall role of the public sector in doing what it should do best: finding criminals and terrorists. Also, the current system of divided responsibilities makes the use of empirically based analytical tools like regression or discriminant function analysis both difficult (by dividing data bases) and unlikely (because the private sector has few incentives to spend the money to do so). These problems can be addressed by turning all analytical work to public sector financial intelligence units and reserving for the private sector only the reporting of objective information: certain client profiling data and records of all financial transactions. Financial intelligence should be required to use, to the extent possible, empirical analysis, results should be far better than the current system. While such a system would be substantially different from the current one, there is considerable precedent in the way in which modern tax administrations select taxpayers for audit investigation. A careful review of key aspects of those systems reveals that the transmittal of only objective information by private parties to tax administrators, and the use of empirically based analytical tools by those administrators to select taxpayers for audit, can work efficiently. In addition to improvements in effectiveness, there should be significant over-all cost savings as redundancies among multiple private sector party analytical duties are eliminated. Both the private sector, which would experience significant cost reductions, and public sector civil servants, who would see an increase in duties and financial support, would be expected to support such changes.
While these changes would entail a larger cost to the public fisc, because this would in part finance greater governmental anti-terrorism work the added public sector costs might be politically acceptable.

INTRODUCTION

Since at least the 1970s there has been a sustained and increasingly global interest in stopping money laundering.\(^1\) The reasons are hardly complex. Law enforcement may be able to follow a money trail of criminal proceeds to find the perpetrator or use the proceeds as evidence in a prosecution.\(^2\) The state may also be able to confiscate the ill gotten gains.\(^3\) Criminals,
therefore, seek to disguise the illegal origins of the proceeds of crime and their ownership of the proceeds.\footnote{4} At least in theory preventing criminals from succeeding makes it harder for them to benefit from their crimes.\footnote{5}

Over the past forty years anti-money laundering rules have been refined a bit, expanded somewhat, but rarely completely re-thought or substantially rewritten.\footnote{6} Today the vast majority of the world’s jurisdictions have endorsed the latest version of the Financial Action Task Force’s [FATF] Forty Recommendations on Money Laundering [FATF 40 Recommendations]\footnote{7} and the FATF 40 Recommendations on Money Laundering, supra note 1 at Recommendation 3, require the adoption of forfeiture laws for the proceeds of crime.

\footnote{4} “When a criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying activity or the persons involved…. In the initial - or placement - stage of money laundering, the launderer introduces his illegal profits into the financial system…. After the funds have entered the financial system, the second – or layering – stage takes place. In this phase, the launderer engages in a series of conversions or movements of the funds to distance them from their source… Having successfully processed his criminal profits through the first two phases the launderer then moves them to the third stage – integration – in which the funds re-enter the legitimate economy.” FATF, Money Laundering FAQ, available at \url{http://www.fatf-gafi.org/document/29/0,3343,en_32250379_32235720_33659613_1_1_1_1,00.html}.

\footnote{5} “Targeting the money laundering aspect of criminal activity and depriving the criminal of his ill-gotten gains means hitting him where he is vulnerable. Without a usable profit, the criminal activity will not continue.” \textit{Id.}

\footnote{6} For example, in the U.S. the first anti-money laundering rule focused on the placement stage (the launderer introduces his illegal profits into the financial system) by requiring financial institutions to identify clients, keep certain client records, and report cash deposits in excess of $10,000. Bank Secrecy Act, \textit{supra} note 1. Future laws extend the definition of financial institutions, enhanced record-keeping rules, and added a requirement to monitor client activity and report suspicious activities. FinCEN, History of Anti-money Laundering Laws, \textit{supra} note 1. Since the FATF’s first set of 40 Recommendations on Money Laundering the definition of financial institution has been extended (and certain requirements have been extended to include some persons who are not financial institutions) and rules on record-keeping have been tightened, but the general framework of client identification, recordkeeping, client monitoring, and reporting of suspicious activities has not changed. FATF 40 Recommendations (1990) and FATF 40 Recommendations (1996), \textit{supra} note 1 at Recommendations 11-15; FATF 40 Recommendations (2003), \textit{supra} note 1 at Recommendations 5-16.

\footnote{7} According to the FATF 130 countries have endorsed the 40. \textit{Id. at Introduction}. In 2002 the International Monetary Fund [IMF] endorsed the FATF 40 Recommendations (and the FATF VIII Special Recommendations on Terrorist Financing (2001), which were amended in 2004 to include Special Recommendation IX, \textit{available at \url{http://www.fatf-gafi.org/dataoecd/8/17/34849466.pdf}}). IMF Advances Efforts to Combat Money Laundering and \textit{Terrorist Finance}, Public Information Notice No. 02/87, August 8, 2002, \textit{available at \url{http://www.imf.org/external/np/sec/pn/2002/pn0287.htm}}; INTERNATIONAL MONETARY FUND, 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 1 (2002), \textit{available at \url{http://www.imf.org/external/np/mae/aml/2002/eng/110802.pdf}}. Because nearly every country in the world is a member of the IMF this endorsement has significant resonance. IMF Members’ Quotas and Voting Power, and IMF Board of Governors, \textit{available at \url{http://www.imf.org/external/np/sec/memdir/members.htm}}. More importantly, each member of the FATF and each of the eight FATF associate members and FATF-style regional bodies has endorsed the FATF 40 Recommendations and Special Recommendations on Terrorist Financing the as the global standard for anti-money laundering and combating the financing of terrorism. \textit{See} FINANCIAL ACTION TASK FORCE, FATF MEMBERS AND OBSERVERS, \textit{available at \url{http://www.fatf-gafi.org/document/52/0,3343,en_32250379_32236869_34027188_1_1_1_1,00.html}} (providing web links to each FATF associate member and FATF-style regional body); \textit{see also} PAUL ALLAN SCHOTT, REFERENCE GUIDE
accompanying Methodology for Assessment. Since 1990 these standards have require financial institutions to monitor the transactions of their customers and to report to government authorities (known as Financial Intelligence Units [FIUs]) those they believe might involve the proceeds of crime (and since 2001, the financing of terrorism). Since the inception of this standard millions of these so-called suspicious activity (or transaction) reports have been forwarded to FIUs by financial institutions. Each year since the inception of standardized system in 2002, assessments of compliance with these anti-money laundering and terrorism financing preventive measures are undertaken by organizations such as the FATF, regional anti-money laundering groups, and the International Monetary Fund [IMF] and the World
Failure to comply can result in countries applying sanctions or countermeasures, including bans on doing business with financial institutions located within their borders.\textsuperscript{15} They are among the most followed global governance standards in the world.\textsuperscript{16} The only major problem is that they don’t work, or at least don’t work very well.\textsuperscript{17}

This Article argues that those anti-money laundering and terrorism financing standards designed to prevent criminals from abusing the financial system need to be rethought. The Article suggests that the long-accepted view that such a significant amount of criminal law enforcement should be left in private hands\textsuperscript{18} is wrong. Instead, it argues that the government should assume from financial institutions the key role they currently play in deciding if their clients are possible money launderers. The Article argues that financial intelligence units should make such determinations in ways that are analogous to how some advanced country revenue authorities select income tax returns for audit, particularly the United States Internal Revenue Service. Financial institutions, the Article suggests, should be relegated to reporting to financial institutions.\textsuperscript{14}

\begin{footnotesize}
\begin{enumerate}
\item For example, Title III, Sec. 311(a) of the USA PATRIOT ACT, Pub.L. 107-56 (2001), 31 U.S.C. § 5318A(b)(5), the Secretary of the Treasury may prohibit, or impose conditions upon, the opening or maintaining in the United States of a correspondent account or payable- through account by any domestic financial institution or domestic financial agency for or on behalf of a foreign banking institution, if he determines that the institution is inadequately applying appropriate anti-money laundering/terrorism financing rules. FATF Recommendation 21 states that “Financial institutions should give special attention to business relationships and transactions with persons, including companies and financial institutions, from countries which do not or insufficiently apply the FATF Recommendations... Where such a country continues not to apply or insufficiently applies the FATF Recommendations, countries should be able to apply appropriate countermeasures.
\item Supra notes 7 and 13 and accompanying text.
\item This view has been expressed by many commentators, including governmental and private sector practitioners and academics. Infra at notes ___ and related text.
\item For purposes of this Article “private” includes those financial institutions and other persons subject to requirements under preventive measures for money laundering and terrorism financing that are state owned. This is because their interests are primarily the same as those that are privately owned, especially in contrast to the interests of financial intelligence units and law enforcement.
\end{enumerate}
\end{footnotesize}
intelligence units only objective information on customers and transactions in much the way that
certain third parties must report taxpayer transactions to revenue authorities.

Part I begins by describing the private sector’s role in the preventive measures system,
which is to identify customers, create a profile of their legitimate activities, keep detailed records
of clients and their transactions, monitor their transactions to see if they conform to their profile,
examine further any unusual transactions, and report to the government any suspicious
transactions. Part I continues by examining the effectiveness of this system. Borrowing from
theory concerning the effectiveness of private sector unfunded mandates, it reviews why many
aspects of the system are failing, focusing on the selection of transactions for referral to public
sector financial intelligence units for further examination for possible money laundering or
terrorism financing. Part I then turns to a discussion of a few issues regarding the impact the
system has but that are not related to effectiveness.

Part I then reviews the public sector’s role in the preventive measures system, which is to
assist the private sector in identifying suspicious transactions, ensure compliance with the
preventive measures requirements, and analyze suspicious transaction reports to determine those
that should be investigated. Part I continues by examining the effectiveness of the system. It
reviews why many parts of the system are failing, focusing on the selection of transactions by
financial intelligence units for referral to law enforcement for possible investigation, as well as a
few additional issues. The Part concludes with a summary and analysis, suggesting how flaws in
both private and public roles might be theoretically addressed.

In Part II this Article turns to a brief review of certain current techniques for selecting
income tax returns for audit. After an overview of the system, Part II first discusses the far more
limited role of the private sector in providing tax administrators with information, comparing this
role to that of the private sector in implementing preventive measures. Next, the Part turns to
consider how tax administrators, particularly the U.S. I.R.S., selects taxpayers for audit,
comparing this to role of both private and public sector in implementing preventive measures. In
doing so, it suggests precedent for suggestions as to how flaws in both private and public roles in
implementing money laundering and terrorism financing preventive measures might be
theoretically addressed. Part II concludes with a short summary and analysis that relates these
conclusions to the preventive measures system.
Referring to the analyses in Parts I and II, Part III suggests changes to the current preventive measures standard.

I. PREVENTIVE MEASURES FOR MONEY LAUNDERING AND TERRORISM FINANCING: FAILURES AND SUCCESSES

A. System Overview

The FATF’s 40 Recommendations and the Special Recommendations are designed to “provide an enhanced, comprehensive and consistent framework of measures for combating money laundering and terrorist financing.”\(^{19}\) Together they cover, \textit{inter alia}, the criminalization of money laundering and terrorism financing, the freezing and seizing of criminal proceeds and of terrorism funds, key preventive measures against laundering and terrorism financing for financial institutions and others subject to preventive measures, financial intelligence units, and international cooperation.\(^{20}\) However, since the original 1990 draft the 40 Recommendations have provided the same basic framework for preventive measures for financial institutions.\(^{21}\)

\(^{19}\) FATF 40 Recommendations (2003), \textit{supra} note 7 at \textit{Introduction}.

\(^{20}\) The FATF 40 Recommendations are broken down into 4 groups. These are Group A: Legal Systems, and include the scope of the criminal offence of money laundering (1 and 2) and provisional measures and confiscation (3); Group B: Measures to be taken by Financial Institutions and (certain) Nonfinancial Businesses and Professions to Prevent Money Laundering and Terrorist Financing, and include prohibition on shell banks (4), customer due diligence and record-keeping (including client identification and transaction monitoring)(5-12), reporting of suspicious transactions and compliance (including internal training and audit programs)(13-16), other measures to deter money laundering and terrorist financing (including sanctions for failure to comply with the Recommendations) (17-20), measures to be taken with respect to countries that do not or insufficiently comply with the FATF Recommendations (21-22), and regulation and supervision (23-25); Group C: Institutional and other Measures Necessary in Systems for Combating Money Laundering and Terrorism Financing, and include competent authorities, their powers and resources (including the establishment of a financial intelligence unit)(26-32) and transparency of legal persons and arrangements (33 and 3)4; and Group D: International Co-operation, including implement various treaties (35), mutual legal assistance and extradition (36-39), and other forms of co-operation (40). The IX Special Recommendations include ratification and implementation of UN instruments (I), criminalizing the financing of terrorism and associated money laundering (II), freezing and confiscating terrorist assets (III), reporting suspicious transactions related to terrorism (also required in Recommendation 13) (IV), international co-operation, (pay special attention to) alternative remittance systems (VI), (special rules on) wire transfers (VII), (pay special attention to) non-profit organizations (VIII), and cash couriers (IX). FATF 40 Recommendations and IX Special Recommendations on Terrorist Financing, \textit{supra} note 7.

\(^{21}\) Since 1990 there has been a progressive expansion of those persons who must follow the ‘preventive measures’ provisions in the FATF 40 Recommendations. FATF 40 Recommendations (1990) at Recommendation 5, FATF 40 Recommendations (1996) at Recommendation 5. The current definition of financial institutions includes Financial institutions include any person who engages in the following activities: acceptance of deposits and other repayable funds from the public; lending; financial leasing; the transfer of money or value; issuing and managing
A. Private Sector Role

FATF Recommendations 5 through 13 plus 21 and 22 (and the accompanying relevant materials in the accompanying Methodology for assessment of compliance) set out the part of the preventive measures system that applies to the private sector. These recommendations (and their counterparts in U.S. rules) form a five part requirement: (1) establish and maintain customer identity (including beneficial owner and controller of the legal title holder of the account); (2) create and maintain an up-to-date customer profile; (3) monitor transactions to see if they fit with the customer profile (of transactions that are legitimate); (4) if not, examine further any such transaction to see if it might represent the proceeds of crime or financing of terrorism, including by examining the source of funds; and (5) if so, report the transaction to the financial intelligence unit, along with a description of why the financial institution believes that the transaction is suspicious. Recommendations 18, 19, and 26 through 34 (and the accompanying relevant materials in the accompanying Methodology for assessment of compliance) address both the supervisory system to ensure that the private sector complies with their preventive measures of payment (e.g. credit and debit cards, checks, traveler’s checks, money orders and bankers’ drafts, electronic money); financial guarantees and commitments; trading in money market instruments (checks, bills, CDs, derivatives etc.), foreign exchange, exchange, interest rate and index instruments, transferable securities, commodity futures trading; participation in securities issues and the provision of financial services related to such issues; individual and collective portfolio management; safekeeping and administration of cash or liquid securities on behalf of other persons; otherwise investing, administering or managing funds or money on behalf of other persons; and underwriting and placement of life insurance and other investment related insurance, money, and currency changing. Methodology, supra note 8 at 65-66. Since 2003 most of the preventive measures prescribed for financial institutions have been extended to certain designated non-financial businesses and persons, including casinos (which also includes internet casinos), real estate agents, dealers in precious metals, dealers in precious stones, lawyers, notaries, and other independent legal professionals and accountants, and trust and company service providers. Id. at 62.

22 A working group consisting of the Commonwealth Secretariat, the United Nations Office on Drugs and Crime, the World Bank, and the IMF has drafted a model regulation for the prevention of money laundering and the financing of terrorism (“Model Regulation”) as part of a model law on anti-money laundering and terrorism financing. The Model Regulation implements these FATF Recommendations based on the regulatory frameworks in the UK, Canada, Australia, and Hong Kong. Article 5.1(a)–(e) of the Model Regulation outlines CDD as the “(a) identification of customers, including beneficial owners; (b) gathering of information on customers to create a customer profile; (c) application of acceptance policies to new customers; (d) maintenance of customer information on an ongoing basis; [and the] (e) monitoring of customer transactions.” Model Regulation (2006) (on file with the U.N Office on Drugs and Crime). Article 10 describes a customer profile as being “of sufficient nature and detail . . . to monitor the customer’s transactions, apply enhanced customer due diligence where necessary, and detect suspicious transactions.” Id.

23 If a new customer profile suggests that the customer is opening an account with proceeds of crime are involved the financial institution should go directly to Step 4. Id.
measures requirements and the criminal investigation and prosecution system for state law enforcement authorities.

As shall be seen, the private sector’s role focuses on three basic objectives. The first is to help exclude from the financial system possible criminal, including terrorist, elements. It does this by making financial institutions and others subject to preventive measures identify and profile potential (and periodically existing) customers to screen out possible criminals and terrorists.\(^\text{24}\) The second is to make available to law enforcement financial information that can be used in criminal investigations or as evidence in a prosecution. It does this by requiring the private sector to maintain records of the identity of all clients and of their transactions.\(^\text{25}\) The third is to identify customers who might be criminals or terrorists so that law enforcement can decide whether to investigate and prosecute such persons. It does this by requiring the private sector to monitor customer transactions based on their profiles and report to law enforcement those which raise suspicion that criminal proceeds or terrorism financing might be involved.\(^\text{26}\)

The United States [U.S.] complies with these requirements through statutory and regulatory measures (although it does not extend these requirements to all those designated non-financial businesses and persons as defined in the Methodology), as well as through guidance financial institutions and compliance with statutory and regulatory provisions.\(^\text{27}\) The language used is similar to that found in the Recommendations.\(^\text{28}\) The European Union does so through

\(^{24}\) See discussion infra at notes ___ and accompanying test.

\(^{25}\) See discussion infra at notes ___ and accompanying test.

\(^{26}\) See discussion infra at notes ___ and accompanying test.


\(^{28}\) Id.
both Directives and implementing legislation at the member country level.\textsuperscript{29} The language used is also similar to that found in the Recommendations,\textsuperscript{30} a similarity that seems to be typical in many if not most implementing jurisdictions.\textsuperscript{31}

Experience suggests that while the second objective appears to work rather well, the first may work less well and the third may rarely work at all.\textsuperscript{32}

2. Customer Identification, Customer Profiling, Record-Keeping

Recommendation 5 requires that financial institutions and others subject to preventive measures under Recommendation 12\textsuperscript{33} and 22\textsuperscript{34} identify their customers, including the beneficial owner of a customer account, which, in the case of legal persons (and other legal arrangements such as trusts), includes taking “reasonable measures” to identify the physical persons who own or control the customer.\textsuperscript{35} Although neither the Recommendation itself nor the Methodology uses the term “client profile” Recommendation 5 requires that the financial institution determine “the purpose and intended nature of the business relationship” of a potential (and periodically, of a current) client and a “knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.”\textsuperscript{36} This serves two purposes. First, if a potential client’s identity and profile cannot be established the financial institution “should terminate the business

\textsuperscript{29} Sorcher, \textit{Lost In Implementation}, \textit{supra} note 1 at 404-415.
\textsuperscript{30} Id.
\textsuperscript{31} The author if this article has formally reviewed implementing language in seven jurisdictions and informally reviewed language in 17 others and found language nearly identical to that used in the Recommendations and Methodology. This may be due to
\textsuperscript{32} See infra notes ___ and accompanying text.
\textsuperscript{33} Recommendation 12 extends these requirements to designated non-financial businesses and persons including casinos (which often deal with cash that can be exchanged for chips), real estate agents (in part because real estate is often of high value it is often used as an investment vehicle by launderers) dealers in precious metals (included for similar reasons), lawyers, notaries, and persons who assist in the setting up of trusts and companies (these are often professionals who assist launderers in hiding assets). FATF 40 Recommendations (2003), \textit{supra} note 7 at Recommendation 12.
\textsuperscript{34} Recommendation 22 requires that the principles applicable to financial institutions are also applied to branches and majority owned subsidiaries located abroad to the extent that local applicable laws and regulations permit; where they do not the parent institution is to inform its own supervisors of this fact. \textit{Id.} at 22.
\textsuperscript{35} FATF 40 Recommendations (2003), \textit{supra} note 7 at Recommendation 5. The Methodology allows an exception from this latter requirement in the event the legal person is a public company. Methodology, \textit{supra} note 8 at Criterion 5.9.
\textsuperscript{36} FATF 40 Recommendations (2003), \textit{supra} note 7 at Recommendation 5.
relationship.”\textsuperscript{37} The second purpose is so that future transactions of accepted clients can be measured against this baseline. Specifically, financial institutions must “understand the purpose, intended relationship, and conduct with the customer, and undergo ongoing customer due diligence in the business relationship,” and must undertake a “scrutiny of transactions through the course of the relationship to ensure that the transactions being conducted are consistent with the institution’s knowledge of the customer, its business and risk profile, including, where necessary, the source of funds.”\textsuperscript{38} In the event the financial institution cannot comply it should terminate business relations or not undertake a transaction.\textsuperscript{39} Second, the client profile allows financial institutions and others subject to preventive measures to monitor client transactions to see if they are unusual compared with the profile.

A key development in the 2003 Recommendations was the adoption of an optional risk-based approach for certain preventive measures.\textsuperscript{40} According to the FATF, the adoption of risk sensitivity “involve[s] identifying and categorizing money laundering risks and establishing reasonable controls \textit{i.e.,} risk-based] based on risks identified….”\textsuperscript{41} This risk-based program contrasts with the previous one, where each of the FATF Recommendations was to be implemented objectively regardless of relative risk levels.\textsuperscript{42} During the years when the FATF was considering the adoption of a risk based-approach disagreement tended to arise at least in part between those FATF delegates from a law enforcement background and those from a regulatory, particularly bank regulatory background, with the larger arguing in favor of a risk-based approach.\textsuperscript{43} In general, the banking regulators were used to dealing with concepts of

\textsuperscript{37} Recommendation 18 also forbids financial institutions to transact business with shell banks and “guard against” establishing relations with those that do. \textit{Id.} at Recommendation 18.

\textsuperscript{38} \textit{Id.}

\textsuperscript{39} It should also consider filing a suspicious transaction report to the Financial Intelligence Unit, but is not required to do so. \textit{Id.}

\textsuperscript{40} This had been highly controversial. During this time the author participated in many of the FATF working group meetings concerning adoption of such an approach. The 1996 version of the Recommendations did not include any references to a risk-based approach. The author was present during many of these discussions.


\textsuperscript{42} \textit{FATF 40 Recommendations (2003), supra} note 7.

\textsuperscript{43} FATF member jurisdictions are represented at the FATF by sub-state units, including regulatory authorities (most particularly banking supervisors), as well as law enforcement.
risk while law enforcement was not. According to the FATF, the new focus on risk allows financial institutions and supervisory authorities to be more efficient and effective in their use of resources and minimize burdens on customers. FATF Recommendation 5 now allows financial institutions to determine the “extent of such measures on a risk-sensitive basis, depending on the type of customer, business relationship or transaction,” and provides examples of both higher risk categories requiring enhanced due diligence and lower risk categories requiring less. The Methodology goes on to provide certain examples of higher risk categories.

Recommendation 6 singles out a particular category of customers, those individuals who are or have been entrusted with prominent public functions in a foreign country, as well as family members or close associates, which are termed politically-exposed persons. The Recommendation requires financial institutions and others subject to preventive measures to have risk management systems to determine if customers are politically-exposed persons and to take reasonable measures to establish the “source of wealth and source of funds” and to “conduct enhanced ongoing monitoring of the business relationship.” In other words, if a customer is a politically exposed person the financial institution and others subject to preventive measures must always take measures to establish the source of funds. Neither the Recommendation nor the Methodology reveals how “enhanced” monitoring differs from the “regular” monitoring of Recommendation 5. Recommendation 6 was added in 2003 to address a perceived public

---

44 “Supervisors must be satisfied that banks and banking groups have in place a comprehensive risk management process (including Board and senior management oversight) to identify, evaluate, monitor and control or mitigate all material risks,” BASEL COMMITTEE ON BANKING SUPERVISION, CORE PRINCIPLES FOR EFFECTIVE BANKING SUPERVISION, Principle 7 (2006), available at http://www.bis.org/publ/bcbs129.pdf. The Core Principles are a framework of minimum standards for sound supervisory practices and are considered universally applicable. Id. at 2. The Basel Committee was established in 1974 by the central bank governors of the G-10: Belgium, Canada, France, Germany, Italy, Japan, the Netherlands, Sweden, the United Kingdom, and the United States. BASEL COMM. ON BANKING SUPERVISION, BANK FOR INT’L SETTLEMENTS, THE HISTORY OF THE BASEL COMMITTEE AND ITS MEMBERSHIP 1 (2009), http://www.bis.org/bcbs/history.pdf?noframes=1. The Core Principles Risks may include credit, concentration, liquidity, operational, business/event, reputational, and compliance. INTERNATIONAL FISCAL CORPORATION, ORGANIZATION OF RISK MANAGEMENT FRAMEWORK IN BANKS: KEY PRINCIPLES (2006).

45 FATF, GUIDANCE ON THE RISK-BASED APPROACH, supra note 62 at 2.

46 FATF 40 Recommendations (2003), supra note 7 at Recommendation 5.

47 Methodology, supra note 8 at Criteria 5.8 and 5.9.

48 Id. at 69.

49 Id.
backlash against developed country banks laundering the proceeds of developed country dictators.\textsuperscript{50} Interestingly, domestic officials and their associates were not included.

Recommendation 7 requires special due diligence with respect to cross-border banking, including obtaining approval from senior management before establishing new correspondent relationships.\textsuperscript{51} Recommendations 8 and 9 relate to new technologies and reliance on third parties for due diligence.\textsuperscript{52}

Recommendation 10 requires that financial institutions maintain customer records, including identification records and transaction records sufficient to permit reconstruction of individual transactions sufficient for evidence in a prosecution, and that these records be maintained for at least 5 years and be available for inspection by competent authorities\textsuperscript{53} (Special Recommendation VII provides more detail with respect to wire transfers).\textsuperscript{54} This, along with Recommendation 5, allows investigative and prosecutorial authorities to “follow the money” of criminal suspects. The United States has put in place similar rules.\textsuperscript{55}

3. Transaction Monitoring and Suspicious Transaction Reporting

Recommendation 11 requires that financial institutions pay “special” attention to “complex and unusually large or unusual patterns” of transactions with no “apparent” economic or visible lawful purpose, examine “as far as possible” the background and purpose of such transactions, and establish the findings in writing\textsuperscript{56} (this requirement is separate from

\textsuperscript{50} The author was present during the initial FATF discussions concerning language that eventually became Recommendation 6.
\textsuperscript{51} \textit{Id.} at Recommendation 7.
\textsuperscript{52} Under FATF 8, financial institutions “should pay special attention to any money laundering threats that may arise from new or developing technologies” and requires that they have “policies and procedures in place” to address any specific risks associated with non-face to face business relationships or transactions. \textit{Id.} at Recommendation 8. FATF 9 permits financial institutions to rely on third parties to undertake some due diligence measures in certain cases. \textit{Id.} at Recommendation 9.
\textsuperscript{53} FATF 10 requires financial institutions to keep and maintain client account records, and that they “must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal activity.” \textit{Id.} at Recommendation 10. ‘Competent authorities’ refers to all administrative and law enforcement authorities concerned with combating money laundering and terrorist financing, including the financial intelligence unit and supervisors. Methodology, \textit{supra} note 8 at page 62.
\textsuperscript{54} FATF Special Recommendations (2003), \textit{supra} note 7 at Special Recommendation VII.
\textsuperscript{55} FFIEC Manual, \textit{supra} note 57 at 21, 118–22, 261–64.
\textsuperscript{56} FATF 40 Recommendations (2003), \textit{supra} note 7 at Recommendation 11.
Recommendation 5’s requirement for ongoing customer due diligence with respect to “scrutiny of transactions.” Recommendation 13 requires that a financial institution report promptly to the governmental financial intelligence unit if it “suspects” or has “reasonable grounds” to suspect, that funds are the proceeds of a criminal activity, which the methodology further defines as filing a suspicious transaction report (Special Recommendation IV includes terrorism financing). Recommendation 21 requires “special attention” to business relationships and transactions with persons from countries which do not or insufficiently apply the FATF Recommendations (although it does not say how this is to differ from non-special attention). It is these Recommendations, along with 5, that create the system requiring financial institutions and others subject to preventive measures to monitor customer transactions based on their profiles and report to law enforcement those which raise suspicion that criminal proceeds or terrorism financing might be involved.

Again, U.S. rules comply with these requirements (except for Recommendation 12; U.S. rules only extend to casinos).

Finally, recommendation 14 protects financial institutions from any liability for filing suspicious activities reports and prohibits any tipping off that such reports are being made, while 15 requires financial institutions develop anti-money laundering programs internal policies, procedures and controls, including compliance management arrangements, internal training, and audit capacities. Recommendation 16 extends most of these requirements to the same designated non-financial businesses and persons as found in Recommendation 12. Again, U.S. rules comply with these requirements (except for Recommendation 12; U.S. rules only extend to casinos).

An essential aspect of this part of the preventive measures system should be emphasized. The first is that financial institutions and others subject to preventive measures must design and implement their own systems. While the five part requirement describes what these systems

---

57 Id.
58 Id.
59 FATF Special Recommendations (2003), supra note 7 at Special Recommendation IV.
60 31 CFR § 103.18 to .19 (2007).
61 FATF 40 Recommendations (2003), supra note 7 at Recommendations 14, 15.
62 Id. at Recommendation 16.
63 31 CFR § [to be added] (2007).
64 See, e.g. Recommendation 5: “Financial institutions should undertake customer due diligence measures…. but may determine the extent of such measures on a risk sensitive basis;” Recommendation 6: “financial systems should
are supposed to accomplish they do not provide any detail as to how they are supposed to do it. For this reason, it is not clear exactly how financial institutions and others subject to reporting requirements should implement those requirements. An exception to this is Recommendation 25, which requires that government authorities establish guidelines and provide feedback to assist financial institutions and others subject to preventive measures, in particular “in detecting and reporting suspicious transactions.”

Both how governmental agencies provide guidelines and feedback, and how the private sector implements its preventive measure requirements, are discussed below.

B. Public Sector Role

1. Overview

Recommendations 18, 19, and 26 through 32 (and the accompanying relevant materials in the accompanying Methodology for assessment of compliance) address both the supervisory system to ensure that the private sector complies with their preventive measures requirements and the criminal investigation and prosecution system for state law enforcement authorities. As shall be seen, the public sector’s role focuses on three basic objectives. The first is to ensure

have appropriate risk management systems;” Recommendation 7: “financial institutions should have policies and procedures in place to address any specific risks associated with non-face to face business relationships or transactions;” Recommendation 8: “financial institutions and other designated non-financial persons and businesses must develop and implement their own systems to carry out their detection, examination, and reporting requirements;” Recommendation 9: a “financial institution should satisfy itself that the third party is regulated and supervised for, and has measures in place to comply with CDD requirements in line with Recommendations 5 and 10;” Recommendation 10: “records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved if any) so as to provide, if necessary, evidence for prosecution of criminal activity;” Recommendation 11: “[f]inancial institutions should pay special attention to all complex, unusual large transactions… [t]he background and purpose of such transactions should, as far as possible, be examined, the findings established in writing, and be available to help competent authorities and auditors;” Recommendation 12: “[i]f a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing it should be required to report promptly its suspicions;” Recommendation 15: “[f]inancial institutions should develop programs against money laundering and terrorist financing…. [including] [t]he development of internal policies, procedures and controls, including appropriate compliance management arrangements….” FATF 40 Recommendations (2003), supra note 7 at Recommendations 5-12, 15.

65 FATF 40 Recommendations (2003), supra note 7 at Recommendation 25.

66 Recommendations 18 and 19 are listed under the preventive measures section of the FATF Recommendations, 26 through 32 are under “C. Institutional and other Measures Necessary in systems for Combating Money Laundering and Terrorist Financing: Competent authorities, their powers and resources.”
the private sector’s compliance with their preventive measure responsibilities. Essentially, governmental authorities must advise, supervise, and regulate financial institutions and others subject to preventive measures to ensure compliance with them though both a guidance and an examination function and though the application of sanctions. The second is to ensure that suspicious transaction reports lead to the investigation of appropriate cases of suspected crime and terrorism. Essentially, a financial intelligence unit receives and analyzes these reports along with other key information, and identifies appropriate cases for investigation. These cases are then forwarded to the appropriate government agency (typically the police), who may decide whether and how to go forward. The government may then choose to prosecute appropriate cases.

2. Guidelines, Feedback, and Supervision

Recommendation 25 requires that government authorities establish guidelines and provide feedback to assist financial institutions and others subject to preventive measures, in particular “in detecting and reporting suspicious transactions.” The Methodology goes further by stating that authorities should provide a description of money laundering and terrorism financing techniques and methods and any additional measures to ensure that the systems implemented by financial institutions and others subject to preventive measures are effective, including information on current techniques, methods and trends (typologies), examples of actual money laundering cases, and case by case feedback, including if a suspicious transaction report was found to relate to a legitimate transaction. The U.S. also complies, to a certain extent, with these requirements.

---

67 See discussion infra at notes ___ and accompanying text.
68 See discussion infra at notes ___ and accompanying text.
69 FATF 40 Recommendations (2003), supra note 7 at Recommendation 25.
70 Methodology, supra note 8 at criteria 25.1-25.2.
71 “The methods used for laundering money and the financing of terrorism are in constant evolution. As the international financial sector implements the FATF standards, criminals must find alternative channels to launder proceeds of criminal activities and finance illicit activities. The FATF identifies new threats and researches money laundering and terrorist financing methods. FATF Typologies reports describe and explain the nature of these methods and threats, thus increasing global awareness and allowing for earlier detection.” FATF, Methods and Trends, http://www.fatf-gafi.org/pages/0,3417,en_32250379_32237202_1_1_1_1_1,00.html.
72 See supra notes supra notes.
In order to ensure compliance with the preventive measures, Recommendation 23 requires that financial institutions be subject to adequate regulation and supervision to ensure implementation of the preventive measures, while Recommendations 29 and 17 require that supervisors have adequate powers to ensure compliance including the imposition of “effective, proportionate and dissuasive sanctions.”

U.S. laws also comply with these requirements, and significant fines, as well as other supervisory and regulatory orders against financial institutions, have resulted.

The efficacy of these efforts and the resulting techniques that the private sector uses to implement preventive measure requirements, are discussed below.

3. Suspicious Transaction Analysis and Referral for Investigation

Recommendation 26 requires that countries establish a financial intelligence unit that serves as a national centre for the receiving, analysis, and dissemination of suspicious transaction reports and other information regarding potential money laundering or terrorist financing. It further states that the financial intelligence unit should have access, directly or indirectly, on a timely basis to the financial, administrative, and law enforcement information that it requires to properly undertake its functions, including the analysis of suspicious transaction reports.

---

73 FATF 40 Recommendations (2003), supra note 7 at Recommendation 23. Recommendation 24 extends this requirement to designated non-financial businesses and persons. Id. at 24.

74 Id. at Recommendations 29, 17.

75 31 CFR 103, 17 CFR 240.17a, 1.32-37.

76 Since September 11, FinCEN has imposed a number of fines on banks for failing to meet its reporting requirements. Moreover, those fines have been extraordinarily large. ABN AMRO, a large European bank, has been hit with a $30 million fine (and more from state regulators). Western Union has also been hit with a $30 million fine for its record-keeping failures. And the Department of Justice has brought criminal prosecutions for anti-money-laundering violations, which resulted in a $50 million civil monetary penalty against AmSouth and $43 million in combined criminal and civil fines against Riggs Bank, which put the bank out of business (footnotes omitted).” David Zaring & Elena Baylis, Sending the Bureaucracy to War, 92 IOWA L. REV. 1361, 1414-15 (2007) [hereinafter Zaring & Baylis, Bureaucracy to War].

77 The line between what some countries formally refer to as their financial intelligence unit and other law enforcement agencies is often blurry. IMF, FINANCIAL INTELLIGENCE UNITS, supra note 56. This article refers to the financial intelligence unit using a functional definition.

78 FATF 40 Recommendations (2003), supra note 7 at Recommendation 26. For example, FinCEN has access to numerous data bases. These include several databases of criminal reports sourced from the Immigration and Customs Enforcement’s TECS II system, the FBI’s National Criminal Information Center, the Drug Enforcement Administration’s Narcotics and Dangerous Drugs Information and NDIC Systems, the United States Secret Service database, and the United States Postal Inspection Service. It also has access to the Office of Foreign Assets Control’s list of Specially Designated Nationals, the Social Security Administration’s Death Master File, and the
Recommendation 10 states competent authorities (including financial intelligence units) should have access to records kept by financial institutions and others subject to preventive measures. Finally, Recommendation 40 states that countries should ensure that their competent authorities (which includes financial intelligence units) provide the widest possible range of international co-operation to their foreign counterparts, of information relating to money laundering, providing that controls and safeguards are in place to ensure that information exchanged is used only in a manner consistent with obligations concerning privacy and data protection. The Methodology further states that financial intelligence units should be authorized to allow foreign intelligence units to search their own databases, including law enforcement databases, public databases, administrative databases and commercially available databases. The U.S. largely complies with these requirements.

Perhaps surprisingly this is the only substantive Recommendation relating to a key policy goal of the preventive measures section (the Methodology adds little).

A few other key recommendations relate to the implementation of preventive measures. Potentially the most important are 33, which requires that countries “ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities,” and 34, which requires that countries also ensure that there is adequate, accurate and timely information

State Department’s list of Designated Foreign Terrorist Organizations. It also has access to commercial database services from organizations such as Dun & Bradstreet, LEXIS/NEXIS, and credit bureaus as well as commercially available lists of “ Politically Exposed Persons.” FinCEN also maintains its own database of investigations and queries conducted through FinCEN’s systems. FinCEN, Feasibility of a Cross-Border Electronic Funds Transfer Reporting System Under the Bank Secrecy Act 9 (October 2006), available at http://www.fincen.gov/news_room/rp/files/CFBFTFS_Complete.pdf [hereinafter FinCEN, Cross-Border Electronic Funds].

79 FATF 40 Recommendations (2003), supra note 7 at Recommendation 10.
80 FATF 40 Recommendations (2003), supra note 7 at Recommendation 40.
81 Methodology, supra note 8 at Criterion 40.4.1.
83 Following the terrorist attacks of September, 2001, staff at the IMF produced the first draft of a methodology for assessment of the 40 Recommendations and (then) VIII Special Recommendations. The draft methodology included a significant number of criteria spelling out in detail the duties of financial intelligence units, including most of those described in infra notes ___ and accompanying text. However, during a meeting in Basel in February, 2002 representatives of the Egmont Group, an informal association of financial intelligence units (see http://www.egmontgroup.org/) objected to the spelling out in such detail of the purposes and activities of FIUs because of the difficulty of finding consensus on such a large amount of detail from such a large group. Nevertheless, the representatives largely concurred that the criteria in the methodology described “an effective” financial intelligence unit. The author of this Article was the principal author of those criteria and was present during that meeting.
on express trusts, including information on the settlor, trustee and beneficiaries.\(^\text{84}\) Obviously these Recommendations relate to the customer identification requirements of Recommendation 5. However, Recommendations 33 and 34 are highly problematic in countries like the United States where information on beneficial ownership or trust relations are not kept by government agencies.\(^\text{85}\) Another potentially key recommendation is Special Recommendation VIII, which states that countries “should review the adequacy of laws and regulations that relate to entities that can be abused for the financing of terrorism.” It goes on to state that “non-profit organi[z]ations are particularly vulnerable, and countries should ensure that they cannot be misused…by terrorist organi[z]ations posing as legitimate entities.”\(^\text{86}\) The finally, Recommendation 18 forbids the licensing of shell banks.\(^\text{87}\)

**C. Private Sector Successes and Failures**

1. Overview

There are a number of considerations relating to the privatization of preventive measures. The most important is the effectiveness of implementation, which will be discussed first. Other issues unrelated to effectiveness will be discussed after.

There have been very few complaints about implementation of record-keeping requirements.\(^\text{88}\) This is less true of the customer identification\(^\text{89}\) and profiling requirements\(^\text{90}\)

\(^{84}\) FATF 40 Recommendations (2003), *supra* note 7 at Recommendations 33 and 34.


\(^{86}\) FATF 40 Special Recommendations (2003), *supra* note 7 at Recommendation VIII.

\(^{87}\) FATF 40 Recommendations (2003), *supra* note 7 at Recommendation 18.

where implementing rules have often been found to be inadequate or where effectiveness has been difficult to determine. The doubts can be based both on the effectiveness of the system as designed by the FATF Recommendations and on how that system is implanted. This is particularly true with respect to monitoring and suspicious transaction reporting requirements, where there have been serious doubts as to whether they actually work to help catch money launderers and terrorist financiers. According to some scholars, at least with respect to the U.S. there is little evidence that preventive measures have reduced money laundering. In the US reports lead to few investigations; it appears that most reports are not even reviewed. Statistics collected in the course of FATF mutual evaluations also tend to suggest that relatively few

---


91 Verhelst interview, supra note 1. The overall effectiveness of client identification tends not to be addressed in FATF compliance reports (or only briefly with little information), often because the rules implementing the FATF Recommendations are themselves inadequate. See e.g. U.S. MUTUAL EVALUATION REPORT, supra note (not discussed at all); AUSTRIA MUTUAL EVALUATION REPORT, supra note at 102-103, 105 (not discussed in detail); AUSTRALIA MUTUAL EVALUATION REPORT, supra note at 70 (inadequate rules obviate discussion of their effectiveness); CANADA MUTUAL EVALUATION REPORT, supra note at 129 (inadequate rules obviate discussion of their effectiveness); U.K. MUTUAL EVALUATION REPORT, supra note at 115 (inadequate rules obviate discussion of their effectiveness); HONG KONG CHINA MUTUAL EVALUATION REPORT; supra note at 96-97 (not discussed in detail); See also discussion infra at notes ___ and accompanying text. Based on the author of this article’s considerable personal experience, when rules are adequate reports may fail to address the issue because of the difficulty in determining effectiveness.

92 Verhelst interview, supra note 1. The overall effectiveness of client profiling tends not to be addressed in FATF compliance reports (or only briefly with little information), often because the implementing the FATF Recommendations are inadequate. See e.g. U.S. MUTUAL EVALUATION REPORT, supra note (not discussed at all); AUSTRIA MUTUAL EVALUATION REPORT, supra note at 106 (not discussed); AUSTRALIA MUTUAL EVALUATION REPORT, supra note at 71 (inadequate rules obviate discussion of their effectiveness); CANADA MUTUAL EVALUATION REPORT, supra note at 130 (inadequate rules obviate discussion of their effectiveness); U.K. MUTUAL EVALUATION REPORT, supra note at 116 (inadequate rules obviate discussion of their effectiveness); HONG KONG CHINA MUTUAL EVALUATION REPORT; supra note at 96-97 (not discussed in detail). Based on the author of this article’s considerable personal experience, when rules are adequate reports may fail to address the issue because of the difficulty in determining effectiveness.

93 With respect to client identification and profiling, FATF mutual evaluation reports tend to consider both the efficiency of the system as required and overall effectiveness. With respect to technical issues in implementation see infra notes ___ and accompanying text.

94 FATF mutual evaluation reports tend to consider only the efficiency of the system as required under the Recommendations and not overall effectiveness. Rules implementing the FATF Recommendations rules are themselves often inadequate. See e.g. U.S. MUTUAL EVALUATION REPORT, supra note at ___; AUSTRIA MUTUAL EVALUATION REPORT, supra note at ___; AUSTRALIA MUTUAL EVALUATION REPORT, supra note at ___; CANADA MUTUAL EVALUATION REPORT, supra note at ___; U.K. MUTUAL EVALUATION REPORT, supra note at ___; HONG KONG CHINA MUTUAL EVALUATION REPORT; supra note at ___. With respect to technical issues in implementation see infra notes ___ and accompanying text.

95 Investigations have a failure rate of 99.9%. David Zaring & Elena Baylis, Sending the Bureaucracy to War, 92 IOWA L. REV. 1361, 1413 (2007) [hereinafter Zaring & Baylis, Bureaucracy to War.]

96 Cuellar, Criminal Law, supra note 1 at 323, 378.
successful investigations are developed from suspicious transaction reports.\textsuperscript{95} If reporting helps it may only at the ex post stage, when the authorities can use records to follow the money, not the detection stage.\textsuperscript{96} There is strong indication that many financial institutions do not believe that financial intelligence units or other governmental authorities make much use of suspicious activity reports.\textsuperscript{97} A major complaint is that the reports are simply too numerous with too many false positives to be helpful.\textsuperscript{98} Perhaps most significantly, a common (if private) refrain heard uttered by financial intelligence unit and financial investigator experts at FATF and FATF-style regional organizations and at compliance assessments is that the system of client profiling and monitoring of transactions simply does not work to provide a significant number of effective leads in proceeds of crime or terrorism financing investigations.

In 2001 Professors Ann Seidman, Robert B. Seidman and Nalin Abeysekere outlined a theory of legislative drafting that discussed, inter alia, factors determining how a proposed policy is turned effectively implemented though a particular law or rule.\textsuperscript{99} They identify three broad categories in analyzing whether the person or persons (actor) subject to a legislative mandate will effectively implement that mandate: the actor’s understanding of the relevant rule; the actor’s anticipation of the implementing agency's behavior; and the non-legal constraints and resources of the actor's own environment.\textsuperscript{100} They further these three categories of possible explanations into seven sub-categories (1) the precise wording of the law; (2) the actor’s opportunity to obey the law (3) the person’s capacity to obey the rule, (4) communication of the law to the actor, (5) the actor's incentive to obey or disobey the law, (6) the process by which the actor decides

\textsuperscript{95} See e.g. AUSTRIA MUTUAL EVALUATION REPORT, supra note at; AUSTRALIA MUTUAL EVALUATION REPORT, supra note at; CANADA MUTUAL EVALUATION REPORT, supra note at; U.K. MUTUAL EVALUATION REPORT, supra note at; HONG KONG CHINA MUTUAL EVALUATION REPORT; supra note at.

\textsuperscript{96} Id. at 412.


\textsuperscript{98} See supra notes ___ and accompanying text.

\textsuperscript{99} ANN SEIDMAN, ROBERT B. SEIDMAN & NALIN ABEYSEKERE, LEGISLATIVE DRAFTING FOR DEMOCRATIC SOCIAL CHANGE (2001) [hereinafter SEIDMAN ET AL. LEGISLATIVE DRAFTING].

\textsuperscript{100} Id. at 93.
whether and how to obey the rule, including input, feedback, and decision-making systems by which the actor chooses how to behave in the face of the rule; and (7) the actor’s ideology.101

These categories can be further analyzed by drawing connections among them and further elucidating their meaning. The more a rule is clearly stated102 and objective103 in its construction104 the more clearly it is communicated to the actor. Also, the easier it is for those enforcing the law to ensure effective enforcement. Opportunity and capacity to obey may also be improved through effective input and feedback from enforcement agents as well as from other features. The process by which the actor decides whether and how to obey the rule may be dominated by various incentive effects, including possible sanctions for failure to comply and various economic incentives. Finally, there may be objective reasons of capacity that extend or limit a party’s ability to comply. With respect to the FATF preventive measures, three effects appear to dominate: clarity and objectivity in the standard as supplemented by feedback from implementing agencies and others, economic and regulatory incentive effects, and objective capacity.

This article will now address the three basic components relating to the effectiveness of private sector preventive measures. It will then address other possible benefits and detriments relating to the private sector’s assumption of such duties.

2. Clarity and Objectivity of the Rule

101 Id. at 95. See also Ann Seidman and Robert B. Seidman, Is Legislation an Unprincipled Mess? ITLAM: Drafting Evidence-Based Legislation for Democratic Social Change, 89 B.U.L. REV. 435 454 (2009) [hereinafter Seidman et al., Is Legislation an Unprincipled Mess?]
102 See REED DICKERSON, THE FUNDAMENTALS OF LEGAL DRAFTING 1-7 (1954) (introducing legal drafting and specifically focusing on wording and achieving substantive clarity as means to improving legal instruments, including legislation and constitutions); TOBIAS A. DORSEY, LEGISLATIVE DRAFTER’S DESKBOOK 169-240 (2006) (describing the importance of writing effectively in legislative drafting and emphasizing that "the essence of effective drafting is clear writing"), cited in Id. at n.35. Of course, there are many scholars who question whether language can ever be clear, see Jane S. Schacter, Metademocracy: The Changing Structure of Legitimacy in Statutory Interpretation, 108 HARV. L. REV. 593, 602-03 (1995) (discussing the postmodern view that there may never be clarity in statutory language). The point I make here is that one can be relatively more or less clear, if never absolutely clear.
104 Id. at 454.
As noted earlier, there have been few complaints about implementation of record-keeping requirements.\textsuperscript{105} This should not be too surprising. First, the rules as written are relatively clear and unambiguous. This is far less true of the customer identification and profiling requirements and the monitoring and reporting requirements.

While the Recommendations describe in some detail the five required components (establish customer identity, create customer profile, compare transactions with customer profile, examine those that do not fit, report those that are suspicious), neither they nor the Methodology give much guidance as to exactly how far, and using what criteria, financial institutions and others subject to preventive measures should go in doing so. The recommendations state that financial institutions and others subject to preventive measures must take “reasonable measures” to verify the identity of the beneficial owner such that the financial institution “is satisfied” that it knows who the beneficial owner is, including taking “reasonable measures” to understand the ownership and control structure of the customer.\textsuperscript{106} “Information” on the purpose and nature of the business relationship should be obtained to ensure adequate profiling, as well as “where necessary” the source of funds.\textsuperscript{107} Recommendation 6 requires “appropriate” risk management systems to determine whether the customer is a politically exposed person and that “reasonable measures” be taken to establish the source of wealth and funds.\textsuperscript{108} Recommendation 8 requires the paying of “special attention” to any money laundering threats that may arise from new or developing technologies.\textsuperscript{109} Recommendation 11 requires that “special attention” be paid to transactions which have no “apparent” economic or visible lawful purpose, and that their background and purpose be examined “as far as possible.”\textsuperscript{110} Recommendation 13 requires the reporting of transactions that a financial institution or other person subject to preventive measures “suspects or has reasonable grounds to suspect” that the funds are the proceeds of a

\textsuperscript{105} See supra notes ___ and accompanying text.
\textsuperscript{106} See supra notes 82-83 and accompanying text.
\textsuperscript{107} Id.
\textsuperscript{108} Id. at Recommendation 6.
\textsuperscript{109} Id. at Recommendation 8.
\textsuperscript{110} Id. at Recommendation 11.
criminal activity or are related to terrorist financing. Finally, Recommendation 15 requires “appropriate” compliance management arrangements.

The phrases in quotes, including “reasonable measures,” “is satisfied,” “where necessary,” “appropriate,” “special attention,” “apparent,” “as far as possible,” “suspects or has reasonable grounds to suspect,” are not defined in the Recommendations nor the Methodology. They are anything but clear and objective, giving rise to the likelihood of subjective implementation. Their use does, however, make clear that financial institutions and others subject to preventive measures not only must design and implement their own systems, but that such a process is expected to require considerable subjective judgment. An important aspect of this is the new risk based option. Because client identification and profiling measures may be applied on a risk sensitive basis as is “determine[d]” by the financial institution, financial institutions and others subject to preventive measures have even greater subjective discretion in designing their systems. According to the FATF, such an approach “requires resources and expertise to gather and interpret information on risks, both at the country and institutional levels, to develop procedures and systems and to train personnel. It further requires that sound and well-trained judgment be exercised in the implementation…. It will certainly lead to a greater diversity in practice which should lead to innovations and improved compliance. However, it may also cause uncertainty regarding expectations, difficulty in applying uniform regulatory treatment, and lack of understanding by customers…. (emphasis added). On their face the preventive measures appear subject to significant subjective and discretionary interpretation by financial institutions and others subjected to their requirements.

There is another problem unrelated to the clarity or objective nature of the standard proposed. It is the substantive problem that the transaction monitoring and reporting requirements themselves do not address the question of risk. While the client identification

---

111 Id. at Recommendation 13.
112 Id. at Recommendation 15.
114 See supra notes 61-68 and accompanying text.
115 FATF, GUIDANCE ON THE RISK-BASED APPROACH, supra note 62 at 2.
116 The private sector has also complained about a failure of regulators adequately to endorse a risk-based approach. KPMG, ANTI–MONEY LAUNDERING SURVEY, supra note at 8.
and profiling requirements now include a risk component,\(^{117}\) the monitoring and reporting requirements do not.\(^{118}\) Suspicious transactions will nearly always have relatively different risk rankings (\textit{i.e.} the degrees of likelihood that criminal proceeds are involved), and suspicious transactions will tend to differ with respect to the total amount of criminal proceeds involved. However, the monitoring and reporting requirements do not describe with any precision at what point on the risk continuum financial institutions should identify suspicious transactions (\textit{i.e.}, the continuum stretching from all transactions about which a financial institution may have any suspicion at all to those for which financial institutions have a very strong suspicion). Also, the FATF Preventive Measures do not provide guidance as to whether financial institutions should consider all transactions equally, regardless of the size of the suspected criminal proceeds, or whether they should focus on transactions with relatively larger amounts of suspected criminal proceeds. This makes a real “risk sensitive” system difficult if not impossible to apply.\(^{119}\)

One restriction on this discretion could come from the methods, trends, typologies, and feedback that government authorities are required to provide.\(^{120}\) Methods, trends, and typologies are produced and published by the FATF, FATF associate members and FATF-style regional bodies\(^{121}\) and national authorities, especially Financial Intelligence Units. However, these examples, red flags etc. do not provide guidance on how to interpret terms or to design systems for client profiling, transaction monitoring, and suspicious transaction reporting. Rather, they provide examples of activities that heighten the risk that a particular client or transaction represents the proceeds of crime or terrorism financing. These include guidance on geographical areas or professions that tend to include a higher incidence, typical tactics used by launderers or patterns that indicate a higher risk of laundering.\(^{122}\) The reports simply identify,

\(^{117}\) See supra notes ___ and accompanying text.

\(^{118}\) See supra notes ___ and accompanying text.

\(^{119}\) See supra note 14.

\(^{120}\) See supra notes 89-92 and accompanying text.

\(^{121}\) See supra note 14.

typically through examples, different money laundering or terrorism financing risks or techniques.\footnote{123}{Id.}

For example, FinCEN, the U.S. Financial Intelligence Unit,\footnote{124}{See \textit{supra} note 1.} provides similar guidance,\footnote{125}{Including summaries of law enforcement cases, tips on the preparation and filing of suspicious activity reports, issues and guidance for financial institutions on procedural matters, topics warranting attention and recent court decisions, an industry forum open to financial institutions to outline issues of concern to their community, and a mailbag and feedback section which addresses issues raised by the financial institution industry, such as filing of suspicious activity reports and identification of suspicious activity categories. U.S. \textit{Mutual Evaluation Report}, \textit{supra} note 56 at 150} including what it refers to as “red flags” and other factors indicating a higher risk of money laundering and terrorism finance, primarily based on prior cases.\footnote{126}{FFIEC MANUAL, supra note 57 at Appendix F. While this section is explicitly entitled “Money Laundering and Terrorist Financing ‘Red Flags,’” other sections of the Manual include various examples of money laundering and terrorism financing techniques. \textit{See e.g. id.} at Appendix G.} Feedback on actual cases has been far more problematic.\footnote{127}{\textit{Id.} at 144. Reporting institutions often do not know how information reported to FinCEN is used, if at all. Nicole M. Healy, Edward J. Krauland, Kevin L. Shepherd, Cari Stinebower, Richard L. Fruehauf, William P. Barry, Abraham Wise, Scott Nance, & Tessa Capeloto, \textit{U.S. and International Anti-Money Laundering Developments}, 43 INT'L LAW. 795 (2009) [hereinafter Healy, \textit{U.S. and International Anti-Money Laundering Developments}].} Oddly, FinCEN does not even provide information readily available that might help spell out objectively some of the requirements provided in the Recommendations, such as known havens for money laundering, the names of known “shell” banks, and the names of senior foreign political figures subject to the heightened due diligence rules of Recommendation 6.\footnote{128}{Sorcher, \textit{Lost In Implementation}, \textit{supra} note 1 at 415.}

FinCEN’s methods are by no means unusual. A recent survey of Australia, the U.S., the U.K., France, and other OECD countries suggests that there is little useful information provided by domestic financial intelligence units to financial institutions, especially with respect to identifying typologies, including new money laundering techniques, trends within existing techniques, and the relative identification of more prominent typologies.\footnote{129}{MATTHEW H. FLEMING, UK LAW ENFORCEMENT AGENCY USE AND MANAGEMENT OF SARS: TOWARDS DETERMINING THE VALUE OF THE REGIME 55, 59–60 (2005), \textit{available at} http://www.jdi.ucl.ac.uk/downloads/publications/research_reports/Fleming_LEA_Use_and_Mgmt_of_SARs_June2005.pdf, [hereinafter FLEMING, UK LAW ENFORCEMENT].} Without clear instructions on how to design a preventive measures system and without adequate guidance and feedback, financial institutions and others subject to preventive measures must still face a compliance supervisory process along with the threat of sanctions for non-compliance. Because the details of individual examinations are generally confidential it is
generally difficult to ascertain how the supervisory process determines compliance. FinCEN’s published compliance actions\(^\text{130}\) reveal very little detail as to nature of the preventive measures systems reviewed.\(^\text{131}\) Breaches identified in the actions are clear failures in implementing the most basic of system requirements.\(^\text{132}\) In the course of conducting six assessments of compliance with the FATF Recommendations this author has reviewed hundreds of examination reports of financial institutions by supervisory authorities. As with the published FinCEN compliance actions, with no exception the reports reveal an attention only to basic system requirements. In no cases has the supervisor provided any assistance in designing or redesigning preventive measures systems beyond recommending basic requirements or given any attention to the likely overall effectiveness of the systems in place.

With respect to clarity and objectivity of the rule one would expect financial institutions and others subject to preventive measure requirements to perform relatively well with respect to recordkeeping and less well with respect to client identification, profiling, transaction monitoring, and suspicious transaction reporting. Further discussion on how the private sector implements these requirements in practice is discussed below.

3. Economic and Regulatory Incentive Effects

There are a number of incentive effects which might militate both in favor of and against financial institutions and others subject to preventive measure requirements seeking to implement an effective identification system. First, this Article will review the general question of conflicting incentives applicable in the application of what is, in effect, a form of privatized policing as an unfunded mandate.

\(^{130}\) FinCEN, Compliance Actions, \url{http://www.fincen.gov/news_room ea/}.

\(^{131}\) “The regulated industry has accused FinCEN of assessing the fines randomly and unpredictably and has sought more guidance from the agency on how it decides to assess fines and why it makes them so large.” Zaring & Baylis, \textit{Bureaucracy to War}, supra note \_\_ at 1415.

\(^{132}\) See e.g. In the Matter of Doha Bank, New York Branch (2009-1) (wire transfer monitoring did not extend to multiple transfers, late filing of suspicious activity reports); In the Matter of NY Branch United Bank for Africa (2008-3) (no internal controls) In the Matter of El Noa Noa Corporation (2008-2)(no implementation of written antimony laundering control program).
The assumption of private policing responsibilities\textsuperscript{133} can be undertaken voluntarily because crimes directly affecting them are not being adequately addressed by the public sector, necessitating the spending of resources as self-help.\textsuperscript{134} As a general rule the private, for-profit sector seeks to keep costs to a minimum, in such instances the private sector would chose to assume the costs of law enforcement because the benefits exceed the costs.\textsuperscript{135} Second, participation can be paid for by the public sector;\textsuperscript{136} the latter of which can be accomplished through competitive contracting or though a system of bounty-hunting or rewards for successfully assisting in the investigation or prosecution of a wrongdoer.\textsuperscript{137} Third, the private sector can be forced to take on the costs of private law enforcement by law,\textsuperscript{138} with no compensation for doing so and with penalties for failure adequately to discharge the required duties.\textsuperscript{139} At least at first look, this appears to be the case with all of the preventive measures applicable to the private sector.

\textsuperscript{133} In the Anglo-Saxon world enforcement of the criminal was almost entirely private up until the first half of the 19\textsuperscript{th} century, when the state began to take a dominant role in policing, investigating, and prosecuting breaches of the criminal law. Ric Simmons, Private Criminal Justice, 42 WAKE FOREST L. REV. 911, 921-23 (2007) [hereinafter Simmons, Private Criminal Justice]. Since the American Civil War, however, the reverse, or the privatizing of law enforcement, has proliferated. BRUCE L. BENSON, TO SERVE AND PROTECT 5-7 (1998) [hereinafter BENSON, TO SERVE AND PROTECT]. “Privatizing” a public service can mean both the decision to provide a service and the administrative action to produce the service. Thomas Kolderie (1986), The Two Different Concepts of Privatisation, 46 PUBLIC ADMIN. REV. 285, 286 (1986), quoted in James F. Gilsinan, James Millar, Neil Seitz, James Fisher, Ellen Harshman, Muhammad Islam & Fred Yeager, The Role of Private Sector Organizations in the Control and Policing of Serious Financial Crime and Abuse, 15 J. OF FIN. CRIME 111, 112 (2008) [hereinafter Gilsinan, The Role of Private Sector Organizations]. In this Article “privatized” law enforcement services refers to the second meaning only.


\textsuperscript{135} This presumably would include costs of lobbying, bribing etc. the public to protect the interests of the private actors.

\textsuperscript{136} Gilsinan et alia have referred to this as “the enthusiastic intelligence operative.” Supra note 19 at 144.


\textsuperscript{138} There is no general legal requirement that private actors enforce the laws beyond the crime of misprision of a felony, which requires both active concealment and a failure to disclose a crime. Christopher Mark Curenton, The Past, Present, and Future of 18 U.S.C. § 4: An Exploration of the Federal Misprision of Felony Statute, 55 ALA. L. REV. 183, 185 (2003).

\textsuperscript{139} These are also known as “unfunded private mandates” (as opposed to “intergovernmental” mandates, where a superior level of government requires an inferior level to do something for free). Gregory G. Rapawy, Recent Legislation: Federal Mandate Procedures, 36 HARV. J. ON LEGIS. 571, 572 (1999). Unfunded mandates are also known as “regulatory expenditures,” in that the regulation creates costs on the party mandate to enforce them even if
If the private sector party would see no direct benefit to its contribution to effective law enforcement other than avoiding penalties for non-compliance, the inherent incentive structure in such an arrangement suggests that the private actor will seek to minimize costs.\textsuperscript{140} As part of the goal of spending as little as possible on required duties the private party could seek to interpret those duties as narrowly as possible, meaning as narrowly as can be gotten away with before the cost of sanctions for non-compliance exceeded the savings from not acting.\textsuperscript{141} Certainly the more clearly stated and objective the privatized enforcement requirement the harder it would be for the private party to interpret “down” its duties.\textsuperscript{142} However, any ambiguity would suggest that at least some of the interaction between private and public sectors would involve the former attempting to restrict duties and the latter seeking to expand them. This general incentive structure would suggest that financial institutions and others subject to preventive measure requirements would tend to minimize efforts to create effective systems for identifying beneficial owner and controller.

However, there may be incentives working in the opposite direction. It may be that although they are required to identify beneficial owner and controller in the manner of an unfunded mandate, financial institutions and others subject to preventive measure requirements may have some self-interest in doing so.


\textsuperscript{140} With respect to the mandated privatization of financial regulation, Gilsinan \textit{et alia} have referred to the private purveyors of police services as “The grudging informant.” Gilsinan, The Role of Private Sector, supra note 19 at 113-114.

\textsuperscript{141} Restricting the scope of a regulatory requirement reduces costs. This can be done on one’s own (until one is sanctioned), or by litigation or lobbying to change the rule. Andrew Morriss, Private Actors and the Control of Regulatory Costs (draft of January 2010).

\textsuperscript{142} At the least the public sector would be expected to provide the private actor with “more precise parameters” with respect to the requirement. Gilsinan, The Role of Private Sector, supra note 19 at 114.

\textsuperscript{143} The economist Paul Samuelson originally defined a “public good” (or a collective consumption good) as something “which all enjoy in common in the sense that each individual’s consumption of such a good leads to no subtractions from any other individual’s consumption of that good.” Paul Samuelson, \textit{The Pure Theory of Public Expenditure}, 36 REV. OF ECON. & STATISTICS 387, 389 (1954). “Which all enjoy in common” means that no one can
specific criminal act but to all persons, primarily through deterrence. For this reason, the benefits of self-help are shared through free ridership, once again militating against the private sector spending any money on a mandate beyond the minimum to avoid sanctions.\footnote{144} However, in many instances there may be an overlap between public and private benefits.\footnote{145} While one would expect the private sector to try and control free-ridership by focusing benefits only on themselves, to the extent that such self-help did spill over to those not paying for the service such private law enforcement would still qualify as a public good. In such cases, however, an obvious detriment would be that the private law enforcement would be directed as much as possible towards private rather than public benefits, and would presumably be limited by such motivation.\footnote{146}

Financial institutions and others subject to preventive measures may voluntarily incur the costs of preventive measures for three basic reasons, to avoid concentration risk, reputational risk, operational risk, and legal or regulatory risk.

In banking, concentration risk is defined as excessive exposure to single borrowers or dependence on single depositors,\footnote{147} it exists in both insurance and securities sectors as well.\footnote{148} A key benefit of client identification could be to help financial institutions reduce concentration risk. The extent to which a party would extend costs to identify clients (including beneficial owners and controllers) would be based on a balance of costs to benefits of avoiding such risk. While neither is immediately obvious, at least some self-interested incentive would exist for at least certain types of financial institutions to implement the requirement to identify clients.

\footnote{144}{In a group that provides itself with a public good, a ‘free rider’ is one who contributes little or mothering to the cost of the good while enjoying its benefits as fully as any other member of the group. The free rider problem acts as a disincentive for groups voluntarily to provide public goods unless there is some way to punish or otherwise control free-ridership. Oliver Kim & Mark Walker, \textit{The Free Rider Problem: Experimental Evidence}, 43 \textit{PUBLIC CHOICE} 3, 3 (1984).

\footnote{145}{\textit{Id.} at 339 (quoting abstract of chapter); Joh, \textit{The Forgotten Threat}, \textit{supra} note 22 at 375-83.

\footnote{146}{Ric Simmons, \textit{Private Criminal Justice}, \textit{supra} note 17 at 925.

\footnote{147}{BASEL COM., CUSTOMER DUE DILIGENCE, \textit{supra} note 94 at paragraphs 14-15.

\footnote{148}{International Association of Insurance Supervisors, Glossary, \texttt{http://www.iaisweb.org/index.cfm?pageID=47&vSearchLetter=c##}.

The next form of risk is reputational risk. Banking regulators have long hypothesized that known or assumed use of banks by criminals could result in adverse consequences as customers and investors reacted by shunning the institution. This is known as “reputational risk,” or risk caused by an event or events adversely affecting the reputation of a bank.\textsuperscript{149} Reputational risk also faces other persons, financial and nonfinancial.\textsuperscript{150} Although discussing sanctions against Iran rather than money laundering and terrorism financing \textit{per se}, Stuart Levey, the Under Secretary for Terrorism and Financial Intelligence under President Bush and now President Obama, suggested that "financial institutions want to identify and avoid dangerous or risky customers who could harm their reputations and business" while Treasury Deputy Assistant Secretary Daniel Glaser stated that "rather than comply with just the letter of the law, we have seen many in the banking industry voluntarily go beyond their legal requirements because they do not want to handle illicit business." Therefore, implementation of anti-money laundering and terrorism financing standards by banks could have direct financial benefits by avoiding such reputational risks.\textsuperscript{151}

However, actually demonstrating such reputational risk has proven difficult. Preliminary studies by Professors Michael Levi and Peter Reuter of stock price fluctuations following news stories reporting the use of banks by money launderers have shown no change.\textsuperscript{152} Also, a confidential survey of compliance officers at three financial institutions that were fined by FinCEN for breaching U.S. anti-money laundering regulations indicated no change in customer base following the disclosure of the regulatory action.\textsuperscript{153} While additional research is needed, there is considerable doubt that financial institutions and others subject to preventive measures would weigh heavily concerns over reputational risk.

\textsuperscript{149} "Reputational risk is defined as the potential that adverse publicity regarding a bank’s business practices and associations, whether accurate or not, will cause a loss of confidence in the integrity of the institution." \textsc{Basel Comm. on Banking Supervision; Customer Due Diligence for Banks}, (October 2001), paragraph 11, available at \url{http://www.bis.org/publ/bcbs85.pdf} [hereinafter \textsc{Basel Comm., Customer Due Diligence}.] The loss of high quality borrowers reduces profitable loans and increases the risk of the overall loan portfolio. Depositors may also withdraw their funds, thereby reducing an inexpensive source of funding for the bank. \textsc{Schott, Reference Guide}, \textit{supra} note 7 at II-5.

\textsuperscript{150} \textsc{The Economist Intelligence Unit, Reputation: Risk of Risks} (2005) (arguing that reputation is the most important and difficult task facing senior risk managers).


\textsuperscript{152} Michael Levi Lecture, IMF (Washington DC 2003).

\textsuperscript{153} Telephone survey conducted by the author in 2009.
There is a second issue related to reputational risk: the concern that the profiling, monitoring, and suspicious transaction reporting requirements as outlined in the FATF Recommendations could be effective even if properly implemented.\(^{154}\) If they were not, there would be little reputational risk benefit to spending money to implement them. There is strong indication that many financial institutions do not believe that financial intelligence units or other governmental authorities make much use of suspicious activity reports.\(^{155}\)

The next important form of risk is operational risk, which is defined as the potential for loss resulting from inadequate or failed internal processes, people and systems, or external events.\(^{156}\) Clearly, at least within the standard cost-benefit analytical framework, implementing those aspects of preventive measures that assist in uncovering fraud would be in the best interests of the private party. However, it is difficult to identify publicly available specific information on how financial institutions seek to prevent financial fraud, an issue not addressed in antimony laundering evaluations. A major reason for this is concern by private parties over protecting propriety systems and concern over competition.\(^{157}\) However, insight into anti-fraud client identification and account monitoring can be gained from examining systems provided by third party services. One of the largest advertises a “Dynamic Multidimensional Risk-Weighted Suspicious Activities Detector” to thoroughly monitor all transactions and quickly detect fraudulent activities with the utmost accuracy,” including check fraud, check kiting, ATM fraud, wire transfer fraud, credit card fraud, debit card fraud, stored valued card fraud, commercial loan fraud, consumer loan fraud, mortgage loan fraud, online banking fraud, point of sales fraud, trading fraud, insurance fraud, identity fraud, employee fraud, and vendor fraud. According to promotional materials, the anti-fraud system is capable of sharing the same server and database with its anti-money laundering system, but is different.\(^{158}\)

That being noted, concerns over fraud and over possible money laundering and terrorism financing are by no means the same. In the first instance, the financial institution is the victim;

\(^{154}\) This issue is discussed infra at notes ___ and accompanying text.

\(^{155}\) See supra note ___.

\(^{156}\) B\(\text{ASEL\ COM.},\ C\text{USTOMER D\E\UE D\ILIGENCE},\ supra\ note at paragraph 12.

\(^{157}\) Similar to problems in identifying information on how the private sector implements preventive measures. See infra notes ___ and accompanying text.

\(^{158}\) Guardian Officer, http://www.gv-systems.com/. According to a sales representative, the algorithms for fraud detection and money laundering/terrorism financing detection are “significantly different.” Telephone interview with John Smith (Cleveland OH, February 20, 2010). For a discussion of
in the second case, the financial institution is the medium through which the crime is perpetrated.\textsuperscript{159} The vast majority of criminal proceeds do not involve fraud against banks;\textsuperscript{160} while there are many possible origins of terrorism financing, bank fraud is only one of them.\textsuperscript{161} For that reason, one would expect financial institutions and others to focus not on money laundering or terrorism financing risks, but on those that directly adversely affect them, like fraud.\textsuperscript{162}

A key aspect of any anti-fraud program that relates to preventive measures is the identification and profiling of potential clients and employees to eliminate possible fraudsters. Among the most common form of customer fraud against banks are creditor fraud and wire and check fraud; these are most easily prevented through the use of proper client identification.\textsuperscript{163} In addition, the monitoring of transactions for those that do not fit client profiles could also suggest fraud.\textsuperscript{164}

Detection can also be assisted by sharing doubts about client bona fides with financial intelligence units, whose access to extensive databases including police records, immigration and customs records, tax records, company-formation records vehicle registries, and supervisory findings\textsuperscript{165} make them particularly effective at uncovering patterns among large numbers of complex financial transactions that point to wire and check fraud, credit card fraud, loan fraud, and embezzlement.

\textsuperscript{159} IMF, \textit{Money Laundering Background Paper}, \textit{supra} note ___ at.
\textsuperscript{160} \textsc{Peter Reuter} \& \textsc{Edwin M. Truman}, \textit{The Fight Against Money Laundering} 22 (2004) [hereinafter \textsc{Reuter} \& \textsc{Truman, the Fight}].
\textsuperscript{161} \textsc{Countering the Financing of Terrorism} 91-206 (\textsc{Thomas J. Biersteker} \& \textsc{Sue E. Eckert} eds. 2008).
\textsuperscript{162} "Banks are called upon to identify ‘proceeds of crime’ when all they can concretely observe are account transactions. The issue then for them is to develop criteria capable of identifying deviant dealings…. More sophisticated software provides detailed background information on clients and account movements. These instruments have also set the criteria for defining undesirable clients or atypical financial operations. ‘The problem is that you have to be sure to target what you want to obtain, and adjust the parameters accordingly.” \textit{Gilles Favarel-Garrigues, Thierry Godefroy, \& Pierre Lascoumes, Sentinels in the Banking Industry, Private Actors and the Fight against Money Laundering in France, 48 British J. Crimin.} 1, 10 (2008).
\textsuperscript{163} IMF, \textit{Financial System Abuse, Financial Crime and Money Laundering—Background Paper} 40 (2001), \textit{available} at \url{http://www.imf.org/external/np/ml/2001/eng/021201.pdf} [hereinafter IMF, \textit{Money Laundering Background Paper}]. While there is far less information with respect to other types of financial institutions, preventive measures rules and financial intelligence units have also assisted in uncovering insurance and securities fraud, including insider trading and market manipulation.
This difference is made clearer in when examining the types of reports filed to financial intelligence units. For example, a significant percentage of suspicious transaction reports (which in the U.S. are termed suspicious activity reports) filed with FinCEN are not concerned with money laundering or terrorism financing but with possible fraud.  

While significant additional research needs to be undertaken, there does appear to be some significant possible anti-fraud benefits to financial institutions and others in applying at least some of the preventive measures required under the FATF recommendations, particularly client identification and client profiling, but also transaction monitoring for possible fraud, though not (necessarily) for possible money laundering and terrorism financing.

The last possible risk to be avoided, legal or regulatory risk, arises from the possibility that financial institutions and others subject to preventive measures may suffer enforcement actions such as fines and criminal liabilities for breaching anti-money laundering or terrorism financing laws or regulations. However, this relates solely to involuntary burdens. Therefore, while there might be some marginal direct benefits to financial institutions and others subject to preventive measures via the reduction of reputational risk through effective implementation of preventive measures, it would appear that financial institutions and others subject to preventive measures would perceive no direct benefit to its contribution to effective law enforcement other than avoiding penalties for non-compliance. This relates directly to the issue of financial incentives through the regulatory process.

In sum, while there is strong suggestion that financial institutions and others subject to preventive measures will see risk-reduction benefits from implementing customer identification and profiling rules and fraud-related reporting, and perhaps some from transaction monitoring, there is no congruency for the latter with anti-money laundering transaction monitoring or with anti-money laundering transaction reporting. Given cost considerations, theory would suggest that private actors would keep costs down and benefits up by concentrating on those aspects that benefit primarily fraud efforts rather than anti-money laundering and terrorism financing efforts.

166 Of the reports filed by depository institutions nearly 400,000 were for money laundering and terrorism financing, while around 300,000 related to financial institution fraud. FinCEN SAR Reviews, supra note 12 at 3.
167 BASEL COMM., CUSTOMER DUE DILIGENCE, supra note 94 at paragraph 13.
169 See infra notes ___ and accompanying text.
There are significant costs associated with unfunded mandates of anti-money laundering and terrorism financing preventive measures, many of which also go to the question of capacity to implement such measures. Exactly how much is difficult to quantify. At least with respect to banks, transaction monitoring appears to be the greatest area of expenditure, which given that it appears to have the least possible private benefit (that is, compared to customer identification and profiling) does not bode well for implementation.

An increasing number of instances financial institutions outsource at least some preventive measure duties, particularly review of client names for profiling purposes, transaction monitoring, and suspicious transaction identification, resulting in what commentator has referred to as a “cottage industry of consultants.” Such outsourcing can have advantages, such as reducing costs and improving product through competition. However, smaller institutions may be buying scaled down scaled-down “anti-money laundering lite” software, which may not be a good sign with respect to effectively implementation at that level. At any rate, implementation costs certainly must have a negative effect on implementation when placed into the cost/benefit considerations of financial institutions and others with preventive measures responsibilities.

That being said, unfunded mandates do have the benefit of shifting costs from the public exchequer to the private sector. This can have some benefits as well as some potential downsides that will be discussed at greater length below.

As noted earlier, there are significant potential regulatory incentives to compliance. However, these incentives, based on fines and other forms of compliance action, have (at least so far) been primarily based on failures to implement clearly stated requirements or to implement

---

170 Various attempts have been made, however. According to some estimate U.S. banks spent about $125 million both in 2003 and 2004 to comply. High-end estimates have placed the total costs of compliance at $7 billion in 2003. Zaring & Baylis, Bureaucracy to War, supra note __ at 1413. Presumably these costs have increased. See also Alan E. Sorcher, Sorcher, Lost In Implementation, supra note 1 at 396 (2005) (noting that banks have significantly increased their spending on AML/CFT procedures).

171 KPMG, ANTI–MONEY LAUNDERING SURVEY, supra note __ at 8.

172 Zaring & Baylis, Bureaucracy to War, supra note __ at 1413.

173 Because the purveyors of private services must persuade their customers to purchase from them they have an incentive to offer a better price/quality mix than others BENSEN, TO SERVE AND PROTECT, supra note19 at 27. This suggests greater risk taking and perhaps innovation as well as greater quality control and lower costs of through greater efficiencies. Id.

174 Diligence is Getting Pretty Pricey, supra note __.

175 See supra notes ___ and accompanying text.

176 See supra notes ___ and accompanying text.
much of any preventive measures system at all. None appears to have been based on a results-focuases failure of the system. It should not, therefore, be obvious how these would incentivize those subject to the unfunded mandates of anti-money laundering and terrorism financing preventive measures beyond instituting those clearly stated requirements.

Because of the unclear and subjective nature of the written requirements, often unhelpful guidance and feedback from government authorities, and lack of clear incentives, one would expect that exactly how financial institutions and others subject to preventive measures requirements actually implement them would neither be clear nor uniform. As noted earlier, neither FATF compliance reports nor sanctions reported by supervisory authorities discuss in any detail compliance systems. 177 An important barrier to learning more about how firms implement their preventive measures requirements is a concern over protecting proprietary information in the context of competitive concerns. 178 However, commentators have provided a list of actions that private firms could take to implement their preventive measures duties in the most effective manner possible. 179 This “wish list” is not a description of what firms actually implement, only what they could do assuming cost was no object. Among these is link analysis. 180 Link analysis is a technique used to find associations within data that might have relevance to the particular research question. 181 Linking these pieces of data from multiple sources adds layers of understanding to the behavior that the data represents. Link analysis explores associations or “links” within collections of data. 182 Increasing the number of data sets available increases the

---

177 See supra note ___ and accompanying text.
178 Confidential interviews conducted with compliance officers at numerous financial institutions in the United States, Hong Kong, The British Virgin Islands, and the Philippines over the past five years. See also PricewaterhouseCoopers, Anti-Money Laundering (AML) and Anti-Terrorist Financing (ATF): Case Study, http://www.pwc.com/lu/en/anti-money-laundering/case.jhtml (providing almost no detail on preventive measures system recommended by outside consultant).
180 Vidyashankar et al., Mine Your Way Part 1, supra note ___ at 3; Vidyashankar et al., Mine Your Way Part 2, supra note ___ at 1, 2.
181 Cuellar, Criminal Law, note 1 at 368.
number and types of links that can be identified. There are number of different types of data sets that could be helpful in money laundering or terrorism financing link analysis. First, personal and financial data (including personal and businesses names, addresses, phone numbers, names of beneficial owners and controllers, bank accounts, deposits, funds transfers) would link people and businesses through their financial transactions. For example, this can establish that Person A has a relationship with Company B and Person C.

Next, descriptive links can be established with data bases that describe the type of business activities normally conducted by the persons within the link. Such data includes customer identification/profiles and other information such as found in business directories such a Dunn and Bradstreet. Links to data that include money laundering or terrorism financing indicators, such as law enforcement data, case files, or suspicious transaction reports, can also be made.

Once such descriptive links are established further analysis can examine whether a transaction between identified persons looks unusual or suspicious. For example, if person A has a criminal record or has made past suspicious transactions, payments to Company B or C could raise suspicion of that they constitute criminal proceeds or laundering. This suspicion could be raised further if person owns or controls company B and company B itself has no known business (e.g. it is a shell company). If C has a record as a terrorist or terrorist organization, a suspicion might be raised that the payments were to finance terrorism. Obviously, the greater the amount of (relevant) data and data types, the more extensive will be the link analysis. However, financial institutions and others tasked with implementing preventive measures are restricted in their access to some useful data sets, an issue that will be discussed below in Part 1 section ___.

Such use of descriptive links and analysis is also described as data mining and the use of algorithms. Such algorithms can be based on typical laundering typologies or “red flag” indicators provided by supervisory authorities and the FATF. However, as will be discussed

---

**ELECTRONIC FUNDS.** See also Cuellar, *Criminal Law,* note 1 at 368. Much of the information in the following two paragraphs has been provided by Boudewijn Verhelst. Verhelst Interview, supra note ___.

---

below, such algorithms appear to be based on idiosyncratic judgment to weight and exclude factors rather than empirically sustainable classifications.\textsuperscript{184}

Empirically derived algorithms would be based on regression analysis or discriminant function analysis. Regression analysis is a technique for discovering the relationship between a dependent variable and one or more and one or more independent variables. It explains how the value of the dependent variable changes when one of the independent variables is changed. This change in dependent variable can also be reflected in a probability distribution. Typically, one begins with a hypothesis that the presence and (and magnitude) or a particular factor (the independent variable) is a predictor of something (dependent variable). One then tests the hypothesis using factual data and statistical analysis.\textsuperscript{185} For example, a dependent variable could be ‘the likelihood that money laundering or terrorism financing is involved in a particular transaction.’ The independent variables could then be some quantifiable aspect of the customer or transaction, say, one of the factors found in money laundering or terrorism financing typologies or in the list of “red flags.” A statistical analysis would then show if the hypothesis is correct and indicate the magnitude of relationship between the presence of a ‘red flag’ and the likelihood that there was money laundering or terrorism finance. Multiple independent variables can be statistically combined in non-linear regression analysis to create multi-variable probabilities.

Another way discovering the relationship between a dependent and independent variables is discriminant function analysis. Here, however, the analysis determines which variables discriminate between two or more naturally occurring groups. It also uses a statistical analysis based on empirical data.\textsuperscript{186} For example, the group could be “those who launder money or finance terrorism,” while the variables could be the same typology factors or red flags in the previous example. Multiple variables can be employed and predictor variables can be expressed in magnitudes. Obviously these two analytical techniques would be superior to assessments

\textsuperscript{184} Frederick Schauer, Profiles, Probabilities, and Stereotypes 92-101 (2003) [hereinafter Schauer, Profiles].


\textsuperscript{186} See generally John Poulsen and Aaron French, Discriminant Function Analysis, (undated), http://userwww.sfsu.edu/~efc/classes/biol710/discrim/discrim.pdf (describing discriminant function analysis).
made on human hunches or “idiosyncratic assessments” that have no proven statistical accuracy.\textsuperscript{187}

Especially given that typologies and red flags that supervisory authorities and others provide appear not to be scientific it seems unlikely that private firms, who are primarily concerned about controlling regulatory/legal risk, would themselves use regression analysis. In addition to such an anticipated response to existing incentives, private sector entities lack access to important data sets (to be discussed below at Part 1, section ). Also, managing large sets of data is simply very difficult to do.\textsuperscript{188}

As noted above at least some firms contract out at least part of their customer identification and client monitoring programs to third party service providers,\textsuperscript{189} and a review of some of their programs provides some insight into services offered. For example, some firms assist in customer identification and profiling by providing a risk screening service to check individual or entity names against a comprehensive data set.\textsuperscript{190} Firms can also supply transaction monitoring services. One “monitors and detects” suspicious transactions “across all business lines” using “a fully integrated dynamic and adaptive multidimensional intelligent engine to detect suspicious activities” using “risk modeling” and “risk-based algorithms” to “analyze and investigate suspicious activities effectively and efficiently.”\textsuperscript{191} But as contractors to those primarily responsible for implementing preventive measures, there is little reason to believe that such third party providers firms would be motivated to provide scientifically-based algorithms based on regression or discriminant function analysis. This would only raise costs without providing a service that would further reduce regulatory or legal risk.

Irrespective of what “the best” firms offer, only some firms use such services, and some contract for “lite” versions.\textsuperscript{192} Exactly why some financial institutions and others subject to preventive measures use such systems is not entirely clear. For some firms it could be a form of regulatory/legal risk “insurance;” as long as a well-regarded third party vendor is a contractor it

\textsuperscript{187} \textbf{SCHAUER, PROFILES, supra note __} at 92.

\textsuperscript{188} “Analysis of such huge volumes imposes a huge computational burden…. “ Vidyashankar et al., Mine Your Way Part 2, supra note __.

\textsuperscript{189} See supra note __ and accompanying text.

\textsuperscript{190} http://www.world-check.com/online/.


\textsuperscript{192} Supra note __ and accompanying text.
is likely that supervisors will not sanction firms for non-compliance.\(^{193}\) It could also be that
some firms do see the systems as helping reduce reputational risk.

There is one perhaps unexpected result of at least the way in which private sector entities
perceive of the way in which supervisors will judge their anti-money laundering and terrorism
financing efforts, and that is the number of suspicious transaction reports filed. In short, they
appear to be much too numerous, providing a huge flow of false positives. If a financial
institution is usually sanctioned only for failure to report suspicious transactions (false negatives)
and not for reporting too many that do not turn out to be suspicious (false positives), there will be
an incentive for financial institutions to apply too little scrutiny and to over-report.\(^{194}\) Currently, in
many key jurisdictions, there have been considerable increases in SAR reporting, even though
costs have also increased.\(^{195}\) Because so few of these reports result in actual prosecutions, the
result has been a general flooding of financial intelligence units with essentially “defensive”
suspicious transaction reports.\(^{196}\) This can generate information overload and generally clog the
criminal investigations system with too many false positives.\(^{197}\)

There are a few possible other good and bad negative effects. The fact that the private
sector is likely act based primarily on self-interest (including controlling costs though sanctions

\(^{193}\) Confidential interviews, *supra* note __.

\(^{194}\) *See generally* Elod Takats, *A Theory of ‘Crying Wolf’: The Economics of Money Laundering Enforcement* 4
(International Monetary Fund Working Paper No. 07/81, 2007), *available at*
http://papers.ssrn.com/abstract=979035
(laying out a theoretical argument for increasing filings of defense suspicious activity reports by reporting
institutions).

\(^{195}\) This conclusion is supported by specific studies of the United States and the United Kingdom. *See* Mariano-
Florentino Cuellar, Cuellar, *Criminal Law*, note 1 at 396 (describing increases in SARing in the United States);
STEPHEN LANDER, SERIOUS ORGANISED CRIMES AGENCY, REVIEW OF THE SARS REGIME 13
(2006), *available at*

\(^{196}\) Verhelst Interview, *supra* note __. “There is no indication that FinCEN…the way in which supervisors will
judge their anti-money laundering and terrorism financing efforts, and that is the number of suspicious
transaction reports filed. In short, they appear to be much too numerous, providing a huge flow of false
positives. If a financial institution is usually sanctioned only for failure to report suspicious transactions
(false negatives) and not for reporting too many that do not turn out to be suspicious (false positives),
there will be an incentive for financial institutions to apply too little scrutiny and to over-report.\(^{194}\) Currently,
in many key jurisdictions, there have been considerable increases in SAR reporting, even though
costs have also increased.\(^{195}\) Because so few of these reports result in actual prosecutions, the
result has been a general flooding of financial intelligence units with essentially “defensive”
suspicious transaction reports.\(^{196}\) This can generate information overload and generally clog the
criminal investigations system with too many false positives.\(^{197}\)

There are a few possible other good and bad negative effects. The fact that the private
sector is likely act based primarily on self-interest (including controlling costs though sanctions
avoidance) it may be more likely to commit to a higher level of unethical acts.\textsuperscript{198} One type of unethical act could be profiling. While profiling based on purely statistical analysis of empirical data found in regression or discriminant function analysis would be helpful in determining which customers and transactions are more likely to be involved in criminal activity, profiling based on even informed guesswork is far more likely to result in unfairness.\textsuperscript{199} Given that all typologies reports, red flags and other guidance is based on informed guesswork one can reasonably speculate that there financial institutions are using unscientific profiling to raise due diligence (and due diligence costs) on certain categories of client that may result in reduced access to the financial system by those clients.\textsuperscript{200} One area where there is some evidence that this is happening is with charities. Special Recommendation VIII suggests that charities appeared to be involved fairly regularly in terrorism-financing transactions. This was emphasized repeatedly in reports that could be used as guidance by financial institutions, their supervisors, and law enforcement, including FATF reports and guidance issues by national regulators.\textsuperscript{201} There is no reason to believe that the Recommendation itself or the reports themselves are statistically based.\textsuperscript{202} But if regulated financial institutions and others subject to preventive measures accept that their regulators believe charities are more likely to be supporting terrorist activity, financial institutions may be less likely to accept them as clients, which could reduce charities access to the formal financial system.\textsuperscript{203} There may be other terrorism-related profiling problems based on type of name (for example, Muslim) or location (say, the Middle East).

Next, preventive measures duties must be financed by either by increasing prices the institutions charge clients, reducing net profits, or (most probably) a mix of the two. Higher

\textsuperscript{198} Simmons, Private Criminal Justice, supra note 18 at 304-5.
\textsuperscript{199} SCHAUER, PROFILES, supra note __ at 92-101. Even those who strongly oppose racial profiling for national security purposes do in part because there is no empirical or statistical basis for the profiling. See, e.g., Yevgenia S. Kleiner, Racial Profiling in the Name of National Security: Protecting Minority Travelers’ Civil Liberties in the Age of Terrorism, 30 B.C. THIRD WORLD L.J. 103, 136-140 (2010).
\textsuperscript{200} For example, some anecdotal evidence suggests financial institutions are accepting fewer money service businesses as clients; because they cater primarily to the poor this can have an adverse effect on financial services among poorer people. Confidential Interview, supra note __.
\textsuperscript{201} Gordon, Trusts or Terrorists, supra note __ at 376-77.
\textsuperscript{202} Such reports are based on examples as proffered to the FATF by national financial intelligence units. Verhelst interview, supra note __.
financial institution prices can have significant and adverse public policy effects, such as decreasing access to financial services by low income clients.\textsuperscript{204}

4. Objective Capacity

The issue addressed in this section is the private sector’s capacity or access to information needed for it effectively implement its preventive measures. Whether state authorities like financial intelligence units have such capacity and access is addressed in the next section.\textsuperscript{205}

On the plus side, financial institutions and others have access to a considerable amount of data required for effective implementation of preventive measures. As the original point of access, they can demand, inspect, and copy client identity documents, and because of relative ease of access to certain data to verify such documents detection of false documentation is relatively successful.\textsuperscript{206} They have access to transactions of their own clients and can easily keep records of those transactions.\textsuperscript{207} They may also have access to public data bases such as company registries, business registries (e.g. Dunn and Bradstreet), court records, and conceivably others.\textsuperscript{208}

Finally, financial institutions in particular are expert at how to store money, move it, and guard it.\textsuperscript{209} They can use this information in using link analysis, and such knowledge could be used to help develop hypotheses as to how launderers might hide transactions or beneficial ownership and control.\textsuperscript{210}

\textsuperscript{204} JENNIFER ISERN & DAVID PORTEOUS, AML/CFT REGULATION: IMPLICATIONS FOR FINANCIAL SERVICE PROVIDERS THAT SERVE LOW INCOME PEOPLE (2005) (discussing, \textit{inter alia}, how increased costs due to implementation of AML/CFT regulations may reduce the supply of affordable financial services to low-income persons).

\textsuperscript{205} See infra at notes ___ and accompanying text.

\textsuperscript{206} This is a principal reason that client identification is relatively successful. \textit{See supra} notes ___ and accompanying text.

\textsuperscript{207} This is a principal reason that record-keeping is relatively successful. \textit{See supra} notes ___ and accompanying text.

\textsuperscript{208} Verhelst Interview, \textit{supra} note ___.


\textsuperscript{210} See discussion of link analysis, data mining, and algorithm development \textit{supra} at notes ___ and accompanying text.
However, significant issues concerning lack of capacity and access to data remain. The first involves determining the beneficial ownership and control of legal persons and legal arrangements such as trusts. Companies and trusts are often used for laundering purposes in large part because disguising ownership and control is relatively easy.\textsuperscript{211} Even though Recommendations 32 and 33 require states to provide such information, they are rarely capable of doing so.\textsuperscript{212} As a result, the identification of beneficial owner and controller may not always be completed in a satisfactory fashion.\textsuperscript{213}

Another key issue involves access to sufficient data to perform adequate link analysis. As noted earlier, link analysis depends on the ability to access as much data as possible. The first problem involves transaction data. Financial institutions and others subject to preventive measures are aware only of the transactions of their own clients and not of other clients. If a client engages in a transaction with a client of another person, the chain or link is severed. If financial institutions and others could share data on transactions with every other financial institution this problem could theoretically be solved, but concerns over client confidentiality and proprietary/competitive concerns would make such information sharing difficult at best, especially with respect to foreign firms.\textsuperscript{214} Even if there were no such concerns, the resulting system would mean that every person subject to preventive measures would need access to every other persons’ customer transaction data base. As a result, every private sector entity subject to preventive measures would be performing a link analysis with every customer of every other such entity. The costs of such a bizarrely redundant system would at the very least be highly duplicative.

\textsuperscript{211} See generally FATF, THE MISUSE OF CORPORATE VEHICLES, INCLUDING TRUST AND COMPANY SERVICE PROVIDERS (2006), and sources cited (describing how corporate vehicles, including trusts, can be used to hide beneficial ownership and control, and reviewing how this can be accomplished in various jurisdictions surveyed).

\textsuperscript{212} See e.g. U.S. Mutual Evaluation Report, supra note 5 at ; Austria Mutual Evaluation Report, supra note 29 at ; Australia Mutual Evaluation Report, supra note 20 at ; Canada Mutual Evaluation Report, supra note 22 at ; U.K. Mutual Evaluation Report, supra note 24 at ; Hong Kong China Mutual Evaluation Report; supra note 26 at

\textsuperscript{213} The author of this Article is currently co-leading a study for the World Bank entitled “The Misuse of Corporate Vehicles in Grand Corruption Cases: Unraveling the Corporate Veil.” A review of over 200 cases of money laundering using corporate vehicles and trusts suggests that accurate identification of ownership and control was rarely successful. See Component 1 Analytical Spreadsheets (February 1, 2010), on file with the author of this Article.

\textsuperscript{214} Sharing client information with both domestic and foreign law enforcement authorities is another matter. FATF 40 Recommendations (2003), supra note 7 at Recommendation 40; Methodology, supra note 8 at Criterion 40.4.1.
The second involves access to other data. While it may be possible to arrange access to publically available information on criminal charges and convictions, it would be difficult if not impossible for private sector entities to have access to such data sets as tax records, police records, immigration and customs records, vehicle registries, and supervisory findings.\textsuperscript{215} Also absent would be previously filed suspicious transaction reports. Under the Recommendations such reports are treated as strictly confidential, not only to protect client interests but to ensure that there is no tipping off.\textsuperscript{216}

Next, as discussed earlier, typologies and red flag indicators, however inadequate, may help in designing algorithms, but because those algorithms are not based on appropriate regression or discriminant function-based analysis they are of only limited use. The private sector does not have access to key information required by such an empirical scientific approach. The first and foremost is that they have no (or limited) access to the dependent variable: a higher probability of money laundering or terrorism financing. In fact, a principle complaint of financial institutions and others subject to preventive measures is that they receive no feedback as to whether their suspicious activity reports are false positives (i.e. result in no further investigations, prosecutions, or convictions) or are in any way useful in uncovering criminal proceeds or terrorism financing.\textsuperscript{217} Without this most basic form of feedback it is impossible to determine if an hypotheses about connections between independent variables identified as indicating a higher likelihood of laundering or terrorism finance is accurate.

This relates to a second problem concerning general capacity rather than access to data. While they have expertise in financial transactions, there is no reason to believe that they are

\footnotesize{\textsuperscript{215} Verhelst Interview, supra note \_\_ at .

\textsuperscript{216} Supra note \_\_ at Recommendation 14.

\textsuperscript{217} EUROPEAN COMMISSION, DIRECTORATE-GENERAL JUSTICE FREEDOM AND SECURITY, FINAL REPORT 30, 53 (2007), available at http://ec.europa.eu/justice_home/doc_centre/terrorism/docs/report_01_02_07_with_appendix_en.pdf. See e.g. AUSTRIA MUTUAL EVALUATION REPORT, supra note \_\_ at 144 (no up-to- date guidance); AUSTRALIA MUTUAL EVALUATION REPORT, supra note \_\_ at 90 (inadequate feedback on suspicious transaction reports filed); CANADA MUTUAL EVALUATION REPORT, supra note \_\_ at 262 (no feedback on suspicious transaction reports filed), U.K. MUTUAL EVALUATION REPORT, supra note \_\_ at 148 (no direct feedback); but see HONG KONG CHINA MUTUAL EVALUATION REPORT; supra note \_\_ at 132 (reporting entity told if suspicious transaction report is subject to further investigation and/or analysis; the reporting entity is be advised of the outcome in due course); KPMG, ANTI-MONEY LAUNDERING SURVEY, supra note \_\_ at 8.}
experts in criminal investigations. This raises considerable doubts that they would be able to form the necessary hypotheses between dependent and independent variables, let alone test them.

5. Issues Unrelated to Effectiveness Implementation

On the other hand, there is an obvious benefit to requiring the private sector to take over public sector duties for no fee: costs (especially visible costs) are shifted from the public exchequer. This frequently has political benefits, even if the result is primarily expressed in higher private sector prices. There may be other cost-savings involved in private un-funded mandates. These may have been a motivation behind the setting up of the current system, but a more likely reason is that the private sector has better (or more easily obtainable) access to certain key information than the public sector.

There is one other key issue unrelated to effectiveness of implementation. It appears that private sector persons subject to preventive measures are not very effective in part because they are unable to develop (nor inclined to develop) scientific, empirically-based algorithms that match independent variables with the dependent variable of more likely to concern money laundering or terrorism financing. In part because of this reason, their suspicious activity reports appear to be too numerous (too many false positives) and otherwise of little use to financial intelligence units in ferreting out cases for investigation. What this means is that private sector persons do not know what independent variables trigger investigations. If they did, they would have an extraordinary tool to help money launderers and terrorists change their tactics and patters (i.e. their independent variables) to reduce the likelihood that they would be investigated and, therefore, caught. This could be significant, if unintended, benefit.

D. PUBLIC SECTOR SUCCESSES AND FAILURES

218 Gordon, Trysts or Terrorists, supra note at 737.
219 Though one commentator has suggested that there may be instances where there are overall costs savings with unfunded government mandates. David A. Dana, The Case for Unfunded Environmental Mandates, 69 S. Cal. L. Rev. 1, 36-38 (1995).
220 This is not unique to preventive measures implementation. See, e.g. Fisher, Privatizing Regulation, supra note 33 at 141; William E. Kovacic, Whistleblower Bounty Lawsuits as Monitoring Devices in Government Contracting, 29 LOY. L.A. L. REV. 1799, 1822 (1996).
The principle purpose of the financial intelligence unit is to analyze suspicious transaction reports and other relevant data to establish whether the data contained in the reports provides a sufficient basis to warrant transmitting the file for further investigation or for prosecution. Through examination and analysis the financial intelligence unit attempts to distinguishing truly suspect transactions from those that are only “benignly” unusual. This process usually begins with the receipt of a suspicious transaction report, after which the financial intelligence unit then engages in a two part analysis. In the first part, tactical analysis, the financial intelligence unit looks for additional information on the persons and transactions involved or other elements involved in a particular case to provide the basis for further analysis. A key element of such tactical analysis is link analysis, which has been discussed at length above in the context of transaction monitoring and suspicious transaction reporting. Financial intelligence units typically have available various types of data, including those publically available data bases to which the private sector has access. It can also have access to data bases to which the public has no access, such as tax records, police records, immigration and customs records, vehicle registries, and supervisory findings.

Largely because the private sector has little difficulty in identifying clients and maintaining records of transactions, financial intelligence units have little difficulty in obtaining such records. However, in most instances, these records are obtained only by request. The same is true with respect to similar information from private sector persons in foreign jurisdictions. In other words, these transactions are not part of a data set that is directly accessible to financial intelligence units. This drastically cuts down on information available to financial intelligence units, whether for link analysis or data mining and algorithm development. There are a few exceptions to this general rule. First, although not required under the Recommendations, some jurisdictions, including the United States, Canada, and Australia, as well and developing countries like the Philippines require automatic reporting of

221 Id.
222 SCHOTT, REFERENCE GUIDE, supra note 7 at VII-3.
223 Id. at VII-5 through 6; IMF, FINANCIAL INTELLIGENCE UNITS, supra note at 57-58.
224 See supra note ___ and accompanying text
225 Verhelst Interview, supra note ___
226 FATF 40 Recommendations (2003), supra note 7 at Recommendation 10.
227 FATF 40 Recommendations (2003), supra note 7 at Recommendation 40; Methodology, supra note 8 at Criterion 40.4.1.
228 Discussed infra at notes ___ and accompanying text.
financial transactions to financial intelligence units. One is cash transaction reporting, which requires that certain types of financial institutions or certain designated others report cash transactions greater than a certain amount. There are good reasons for this. In the paradigm case of money laundering, to which anti-money laundering laws were first primarily addressed,\footnote{See supra note __ and accompanying text.} drug traffickers tend to be paid in cash rather than check or credit card, which can be traced. In order to avoid use of large amounts of cash (which can be bulky and can invite unwanted attention) criminal needs to enter the cash into the formal financial system via a financial institution. Doing so is referred to as the “placement stage.”\footnote{SCHOTT, supra note __, at I-7 to I-9.} One of the first AML principles was to require financial institutions (especially banks, which are usually the point of entry in the financial system for cash) to identify exactly who their customers were and to report to the authorities whenever a customer deposited a substantial amount of cash.\footnote{Gordon, Trysts or Terrorists, supra note __ at 708.} The U.S., for example, has long had automatic cash transaction reporting rules for amounts in excess of $10,000, as have a number of other countries.\footnote{Currency Reporting Act, supra note 1. Canada and Australia also require cash reporting.} Another is international wire transactions. A number of jurisdictions, including Canada and Australia, require financial institutions to report to their financial intelligence units either transactions above a certain sum (Canada)\footnote{The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) collects reports related to any cross-border electronic funds transfer in an amount of $10,000 (CAN) or more. See FINTRAC, What Must be Reported? Electronic Funds Transfer, available at \url{http://www.fintrac-canafe.gc.ca/reporting-declaration/Info/rptEFT-eng.asp}.} or all transactions regardless of amount (Australia).\footnote{AUSTRAC, International funds transfer instructions, available at \url{http://www.austrac.gov.au/inter_funds_transfer.html}.} In both cases transactions are reported automatically. An analysis by FinCEN suggested that such data, by extending link analysis, can have significant benefits.\footnote{FinCEN, CROSS-BORDER ELECTRONIC FUNDS, supra note __ at 5-10.} At the same time, it suggests that because of technology advances it would be relatively inexpensive for financial institutions to institute,\footnote{Id. at 21-22.} although it would require the addition of data storage and processing capacity at FinCEN.\footnote{Id. at IV.}

Following tactical link analysis the financial intelligence unit typically undertakes operational analysis. Operational analysis uses tactical information to formulate different
hypotheses on the possible activities of the suspect to produce operational intelligence for use by investigators. It uses:

all sources of information available to the FIU to produce activity patterns, new targets, relationships among the subject and his or her accomplices, investigative leads, criminal profiles, and—where possible—indications of possible future behavior. One of the techniques of operational analysis used in some financial intelligence units is financial profiling.238

Based on such analysis, the financial intelligence unit may or may not disseminate a report for further investigation.239

Another important function of the financial intelligence unit is strategic analysis, or is developing relevant knowledge on techniques of laundering or terrorism financing, such as the identification of evolving criminal patterns in a particular group or the provision of broad insights into emerging patterns of criminality.240 The financial intelligence unit can then use these for its own operational analysis of suspicious transaction reports through linking as well as to develop guidelines, typologies etc. for use by financial institutions and others subject to preventive measure requirements.241

This generally follows he system used by FinCEN in the United States.242

However, like the private sector, financial intelligence units do not use the statistical either regression analysis or discriminant function analysis.243 One of the reasons they may not do so is that regression analysis or discriminant analysis require knowledge of the independent as well as the dependent variables, which at present they do not automatically have access to (although they can request and receive records on specific transactions). Because financial intelligence units do not use these statistical analytical tools methodologies and “red flags” are made on human hunches or “idiosyncratic assessments” that have no proven statistical

---

238 IMF, FINANCIAL INTELLIGENCE UNITS, supra note at 59.
239 Id. at 60.
240 SCHOTT, REFERENCE GUIDE, supra note 7 at VII-3.; IMF, FINANCIAL INTELLIGENCE UNITS, supra note at 59-60.
241 IMF, FINANCIAL INTELLIGENCE UNITS, supra note at 60.
242 U.S. MUTUAL EVALUATION REPORT, supra note 56, at. 126-36.
243 Verhelst Interview, supra note __.
Other failings of financial intelligence units have to do with their interaction with the private sector. They provide inadequate feedback, including assistance in designing preventive measures systems or data on the usefulness of suspicious activity reports, and typologies and red flags are not based on scientific analysis.\textsuperscript{245}

\textbf{E. \textit{Summary and Conclusions}}

While the preventive measures system currently in place has some successes, there are a number of areas of significant failure.

The Recommendations concerning private sector responsibilities are, at least with respect to designing, implementing a profiling, monitoring, and suspicious transaction reporting system, too vague. It is no doubt possible to make the wording somewhat clearer, as well as to improve guidance, feedback, and the application of sanctions. However, it is difficult to see how to make the system itself significantly less subjective and open to interpretation providing that the private sector is to be given the job of design and implementation itself. Also, as long as system design and implementation is an unfunded private mandate, incentives will tend to militate in favor of a less expensive and therefore probably less effective system. In theory it might be possible to pay the private sector by offering bounties for success, meaning for suspicious transaction reports that lead to further investigations, and perhaps to eliminate the perceived safe harbor for filing false positives.

Another theoretical possibility would be to de-privatize the system, turning it over to the public sector to design and implement. By turning all analytical tasks to the public sector, there is no need for the private sector to design or implement a selection system. Doing so would address the problem resulting from the fact that splitting responsibilities among individual private parties and the financial intelligence unit splits up the available data bases used in link analysis. Each individual private party has access to its own client data bases but not to that of any other private party, and concerns over confidentiality, competition, and massive redundancy makes the possibility of sharing such databases highly unlikely. Next, private parties do not have access to confidential data bases that financial intelligence units have. Finally, while

\textsuperscript{244} \textit{SCHAUER, PROFILES, supra note __ at 92}.
\textsuperscript{245} See \textit{supra} notes __ and accompanying text.
financial intelligence units have access to those databases, they do not have access to the various private sector client transaction databases, except in certain instances such as cash or international wire reporting. At least in theory, this problem could be solved, at least with respect to domestic private parties, if the system of link analysis were to be de-privatized and all client identification and financial transactions were to be reported to the financial intelligence unit. It may also be easier to define with clarity and objectivity such a private sector responsibility, obviating many of the problems of subjectivity that currently exist with the current system of privatized obligations. While there would remain some difficulty in confirming beneficial owner and controller, the responsibility for providing much of this data is already primarily a public sector duty.

Turning all responsibilities for monitoring and identifying suspicious transactions to financial intelligence units would also eliminate the need for the private sector to develop expertise in those areas. It would also eliminate the need for the public sector to provide any assistance in designing such systems, or to supervise their implementation.

In order for financial intelligence units to complete operational analysis, however, it would also be necessary for the private sector to convey to them information on client profiles. While identification and transaction records are relatively simple to determine and maintain, profiling is a far more subjective requirement. However, this is due primarily to the fact that exactly what constitutes non-criminal or normative transactions is not spelled out in clear detail. In theory it might be possible to define such a data field with greater accuracy.

Another problem is the failure of both private sector persons and financial intelligence units to use empirically and statistically based on regression or discriminant analysis. Currently the private sector does not have the incentive or the information necessary to do so. The public sector also does not do so, perhaps in part because they do not have access to all the private sector held customer profiling and transaction data that constitutes many of the relevant independent variables. In theory this problem could perhaps be obviated if financial intelligence units were tasked with using scientific methods of regression or discriminant analysis and if they had access to all the data currently not reported to them by the private sector. Once a scientifically derived algorithm is determined, financial intelligence units could complete operational analysis and create reports for immediate referral to investigators. They would
determine themselves the most important parameters, such as likelihood of catching significant
criminal proceeds or terrorism financing.

Key additional benefits of such a system might be avoidance of the problems of non-fact
based profiling and of turning over to the private sector the key to avoiding money laundering
and terrorism financing investigations. One disadvantage is that public sector costs would be
higher, which carries political costs. However, because there would be no redundancy among
the many private parties who now must develop and implement their own systems for client
monitoring there should be a significant overall savings in total implementation costs. Also,
there would likely be significant political support from the financial sector, which would see
significant savings, and also from civil servants who work for financial intelligence units, who
would see duties, including budget support, increase significantly.246 Finally, because the
preventive measures system includes not only money laundering but terrorism financing, it may
be easier politically to increase public funding than it would be for other programs.

II. FAILURES AND SUCCESSES IN SELECTING INCOME TAX RETURNS FOR AUDIT

A. System Overview

This part will focus on these systems in the hope that they will reveal features that may
help better understand the flaws in the current system of anti-money laundering and terrorism
financing preventive measures. Unlike the anti-money laundering system, there is no single
globally determined standard for the design and implementation of tax administrations.247 That
being said, a number of tax authorities from advanced countries, including the United States,
have developed administrative systems that share many features. A key function of these

246 Not surprisingly, public sector unions concerning are typically opposed to growth and aggrandizement of private
sector policing. Stephen Schneider, Privatizing Economic Crime Enforcement: Exploring the Role of Private Sector
Investigative Agencies in Combating Money Laundering, 16 POLICING & SOC. 285, 304 (2006). This would reverse
the process.

247 While the FATF 40 Recommendations and IX Special Recommendations are widely accepted as a global
standard, some features of income tax administration are becoming something like global standards. See Richard K.
501, 584-87, 588-89 (2010).
systems is to improve compliance with revenue laws. While there are many facets to compliance, taxpayer audits are a critical component. In the course of an audit, tax administrations examine a particular taxpayer to determine whether that taxpayer has complied with her or his obligations under the law. A key facet of a tax administration’s audit program is the selection of persons for audit. This Part draws an analogy between the selection of individual income taxpayers for audit by tax administrations and the selection of customers of persons subject to preventive measures for investigation by financial intelligence units.

As discussed in Part I of this Article, the implementation of private sector preventive measures for money laundering and terrorism financing involve two groups. The first consists of private sector financial institutions and certain others who must examine and report on certain activities of their clients. With respect to the tax audit function, however, the private sector consists of two groups: third parties who file reports with the tax authority concerning other taxpayers, and taxpayers themselves who file tax declarations, known as ‘returns’ in the United States. While as currently constituted private sector preventive measures require the private sector to make judgments as to the likelihood that a particular customer has committed money laundering or terrorism financing, those who provide third party information reporting do not. It is the tax administration that makes the decision whether to audit a taxpayer, not the third party.

B. Role of the Private Sector

1. Third Party Reporting

The income tax involves the computation of tax due based, in part, on applying a tax rate to the net of taxable gross income and allowable deductions. Therefore, key aspects of income tax administration include ensuring that all taxable gross income is included and that only allowable deductions are subtracted, and that the proper tax rate is applied to this net. Not surprisingly, income tax administration focuses to a large extent on these items of inclusion and

---


249 Id., at 6

250 Id.
deduction. Third party information returns tend to focus on these items, particularly items of income.

Third party information reporting is a common feature on developed country tax systems.\textsuperscript{251} As with information reporting by persons subject to preventive measures for money laundering and terrorism financing, third parties are not compensated, making the system another example of an unfunded private mandate.\textsuperscript{252} For example, in the United States there is a wide array of third-party information reporting requirements.\textsuperscript{253} U.S payors of wages, interest, or dividend income must report those payments, while brokers must report the amounts realized from securities sales\textsuperscript{254} as well as “a steady stream of updates regarding more arcane items.”\textsuperscript{255}

As is the case with financial institutions and others with private sector preventive measure responsibilities, third party reporters are subject to sanctions for failure.\textsuperscript{256} However, unlike the suspicious transaction reporting system, which requires extensive decision-making in the context of a highly subjective system, the third party reporting system is very objective. All that is required of the third party reporter is to identify the taxpayer, the payment to the taxpayer, and report both to the tax authority.\textsuperscript{257} There are un-compensated costs associated with such requirements. However, the requirements are relatively straightforward, and third party reporters develop expertise with respect to distilling and disseminate this information.\textsuperscript{258} In a manner similar to system whereby some countries require the automatic reporting of cross-border transactions to financial intelligence units, third party reporting can be easily automated, though in these instances often by contracting with data management specialists.\textsuperscript{259} While taxpayers are also required to report income and deductions and are subject to sanctions reporting incorrectly,

\textsuperscript{251} OECD, COMPLIANCE RISK MANAGEMENT, supra note __ at 10-12.
\textsuperscript{252} Steven A. Dean, The Incomplete Global Market for Tax Information, 49 B.C. L. Rev. 605, 613 (2008)
\textsuperscript{hereinafter Dean, The Incomplete Global Market}.
\textsuperscript{253} I.R.C. §§6050A-6050V.
\textsuperscript{254} I.R.C. §§ 6041-42.
\textsuperscript{257} I.R.C. §§ 6043.
\textsuperscript{258} See, e.g., I.R.S Form W-4 (wages) and I.R.S. Form 1099-Int (interest).
\textsuperscript{259} See, e.g., Totally Paperless, http://www.totallypaperless.com/reviews/copanion.html.
they have a direct interest in fashioning their declarations to minimize their liability; taxpayer sanctions are designed in part to counteract this incentive effect. However, third party reporters have very little direct incentive to misreport in the face of possible sanctions.

Finally, unlike with the preventive measures system, the private sector plays no other role in the audit selection system. All analytical tasks, including design and implementation, are assigned to the public sector.

C. Role of the Public Sector

The tax administration authority has the sole responsibility to determine which taxpayers should be audited. Unlike the private sector (and quite possibly the public sector) in the preventive measures systems, tax authorities typically have a specific goal in determining which taxpayers to audit: They generally base their decisions on some estimation of the degree of risk of understatement of tax due multiplied by the size of the understatement. In order to effect such a goal, tax administrations may use a number of techniques. These can include matching third party information with that provided by the taxpayer in a tax declaration, and data-mining with algorithms such as discriminant or regression analysis, and “red flag” analysis.

One would expect details about audit selection strategies to be a well-kept secret; otherwise taxpayers would have a roadmap of how to avoid an audit.

The first is third party information return data matching, which may actually be an exception to the “well-kept secret” rule. This is such an effective technique that in the U.S., whenever there is a discrepancy (above a certain threshold) between information provided in a self-reported tax return information and the information reported by third parties, an automatic notice that taxes are due is sent to taxpayers without bothering to go through the audit process.

---

263 Id. at 583.
first. The U.S. I.R.S. has augmented its data-matching by deriving useful additional material from sources other than third-party reporters. In fact, it is because taxpayers are aware of such a strategy (at least in theory) that the government is receiving third-party information, taxpayers are far less likely to try and cheat with respect to items subject to such reporting.

The next is the use of algorithms such as discriminant or regression analysis, the gold standard for determining the statistical relationship between dependent and independent variables. Apparently far fewer tax authorities use such techniques than data matching (the OECD has identified the U.S. and the U.K.). The U.S. system uses a discriminate function analysis. According to the I.R.S., a Discriminant Function System (DIF) score rates each taxpayer return for the potential for change, based on past IRS experience with similar returns. In particular, an Unreported Income DIF (UIDIF) score rates the return for the potential of unreported income. IRS personnel screen the highest-scoring returns, selecting some for audit and identifying the items on these returns that are most likely to need review. While the I.R.S. has admitted to using such a system, for obvious reasons the process of the analysis is “one of the best kept secrets in government.” However, prior to the institution of the DIF system about half of all IRS audits resulted in no tax change; afterward only one-fifth showed no change (although this fact gives no indication of the change in magnitude of the additional taxes recovered).

Because of secrecy concerns some speculation is required as to the true nature of the program. In order to design a discriminate function one must first formulate a hypothesis about the relationship between dependent variable (risk of understatement of tax (or income?)) multiplied by size of understatement) and possible independent variables; in order to test that

---

265 For example, data on dependents (which can result in deductions from income) are obtained from various government sources. Nina E. Olson, Closing the Tax Gap: Minding the Gap: A Ten-Step Program For Better Tax Compliance, 20 STAN. L. & POL’Y REV 7, 8 (2009).
267 OECD, COMPLIANCE RISK MANAGEMENT, supra note ___ at 14-15, 34-35.
269 Id.
270 Dubin, et ali. The Changing Face, supra note ___ at ___.
hypothesis sufficient data must first be collected. Beginning in 1963 such data was collected through the Taxpayer Compliance Measurement Program, whereby the I.R.S. undertook thorough audits of representative samples of individual income tax returns approximately every three years.\(^{272}\) This program of data collection was apparently abandoned because of the burden placed on those taxpayers who had the bad luck to be selected for audit,\(^{273}\) but it has been replaced with National Research Program (NRP), a data collection program that relies on audit information as well as added data obtained from various government sources, as well as data obtained from public records (e.g., current and prior addresses, real estate holdings, business registrations, and involvement with corporations).\(^{274}\) Obviously, while limited, this system is more scientific than that used either by the private or public sector in implementing suspicious activity reporting and referral of cases for investigation.

While the discriminate function is a secret its number of independent variables is limited. At least in part for this reason, the U.S. IRS does not rely solely on discriminant function analysis to select returns for audit. Like financial institutions and others subject to monitoring and suspicious transaction reporting requirements, the IRS, as well as many developed country tax administrations,\(^{275}\) uses more subjective “red flag” types of reviews.\(^{276}\) While one can assume these are based on experience, one can also assume that they are more imprecise than the more scientific discriminant function analysis.\(^{277}\)


\(^{273}\) Id. at 1263


\(^{276}\) Ronald A. Pearlman, *Demystifying Disclosure: First Steps*, 55 TAX L. REV. 295-96 (2002). Interestingly, this data is not filed by 3rd parties, so there is a direct incentive by the taxpayer to misstate. However, apparently the combination of incentive to cheat against disincentives from sanctions is sufficient that the I.R.S. still picks up significant useful information for its red flags strategy.

\(^{277}\) An indication of “red flags” are items required in Schedule M-1, Raskolnikov, *Crime and Punishment in Taxation*, supra note ___ at 585-9.

\(^{277}\) An indication of “red flags” are items required in Schedule M-1, Raskolnikov, *Crime and Punishment in Taxation*, supra note ___ at 585-9. which requires the corporate taxpayer to reconcile its financial accounting income with the income it reports on its tax return. Some of the information required is general; other detailed. The partnership version of Schedule M-1 does not even require the disclosure of book-tax differences. Even less information is required of an unincorporated sole proprietor on Schedule C to Form 1040. Raskolnikov, *Crime and Punishment in Taxation*, supra note ___ at 585-9.
Apparently in order to make red flag application more standardized and more automated the IRS has developed what they call a Dependent Data-based System. This is a risk identification system powered by rules with each rule identifying “non-compliant indicators” (i.e. red flags); if the rule conditions are met the rule “fires.” Each fired rule receives points based on established scoring methodologies. By 2004 only a few rules has been included, but the IRS stated that it was working to expand the number.\textsuperscript{278} The U.S. also uses other far more general criteria to determine audits; Returns of higher income individuals are examined more frequently than of those with lower incomes, individual taxpayers who earn primarily wage income and take standard deductions face a far lower audit rate, taxpayers with business or farm income face higher chances of an audit than those without it.\textsuperscript{279} It is unknown exactly why the IRS has not expanded its discriminant function system to include more independent variables, but it may have something to do with the considerable expense involved and the lack of support for additional funding for the Internal Revenue Service.\textsuperscript{280}

\textbf{D. \textit{Summary and Conclusions}}

Because the income tax audit system requires private sector entities to report only objective information that can be transmitted electronically, it has a significant advantage over the preventive measures reporting system, supporting the theoretical proposition that such an ‘objective information’ rule be exported to that system. By turning all analytical tasks to the public sector, there is no need for the private sector to design or implement a selection system. This has the benefits of eliminating the need for the private sector to develop expertise in tax administration and audit selection. It also eliminates the need for the public sector to provide any assistance in designing such systems, or to supervise their implementation. It also eliminates virtually all negative private sector incentive effects, including those relating to implementation and non-fact based profiling.

By turning all information and analytical responsibilities to the public sector, which is the sole repository of expertise on non-compliance, it is possible for tax administrations to develop a

\textsuperscript{278} OECD, Compliance Risk Management, \textit{supra} note _ at 15-17.
\textsuperscript{279} Raskolnikov, \textit{Crime and Punishment in Taxation}, \textit{supra} note ___ at 584.
\textsuperscript{280} Confidential Interview, I.R.S. District Director (Cambridge, MA May 1, 1994).
scientifically based system of audit selection. Instead of relying solely on even educated guesses, the discriminant function system guarantees a higher level of correlation between dependent and suspected independent variables of tax non-compliance. This reduces the need for red flag based selection. However, by placing both all expertise and red flag based activities in one entity, greater quality and greater consistency are likely than they would be if split into many entities. This is clearly an advantage over the preventive measures system.

One disadvantage is that public sector costs are higher than they would be if additional duties were turned to the private sector.

III. PROPOSAL FOR A NEW FRAMEWORK FOR PREVENTIVE MEASURES FOR MONEY LAUNDERING AND TERRORISM FINANCING

Based on the above analysis, a rethought system of preventive measures for money laundering and terrorism financing would radically shift the burden from private entities to one public entity. Private sector persons currently tasked with client identification, profiling, record-keeping, monitoring, and suspicious transaction reporting would be tasked with only the first two, plus the transmittal of certain profiling information and of all transactions to financial intelligence units. Client profiling information, however, would be strictly defined; a limited number of data fields would be spelled out by the financial intelligence unit. Transaction data would include all client transactions. All data would, where possible, be transmitted electronically.

Financial intelligence units would be solely tasked with analyzing all data transmitted by financial institutions and others subject to reporting requirements and determining which clients and transactions should be investigated for possible laundering or terrorism financing. They would also be required to determine what their specific goals were in doing so. With respect to laundering, this would be probability of laundering multiplied by magnitude of laundering. With respect to terrorism finance, this might just be probability of financing or some formula of probability multiplied by potential danger of financing. As now, financial intelligence units would be required to send such reports on to law enforcement for investigation.

Financial intelligence units would continue to have access to other sources of information as now. They would also perform standard link analysis, as they do now. However, they would
also be tasked with testing and improving various hypotheses regarding the relationship between independent variables (for example, probability of laundering multiplied by magnitude of laundering; probability of terrorism financing multiplied by potential danger of financing) and possible dependent variables, many of which are now “red flags.” They would use regression or discriminant function analysis. However, because of the resources and time required for such analysis, it would also be understood that such empirical and statistical analysis would be an ongoing project, with additional factors added as research was completed. Because of this, financial intelligence units would continue to use red flag analysis. However, where possible they would automate such analytical work by using rule-based programs such as the I.R.S. Dependent Data-based System.

CONCLUSION

The current preventive measures system does not work well. There are a number of reasons for this. The system requires the private sector to do too many things. Monitoring client transactions and reporting those that raise suspicion of money laundering or terrorism financing is a task for which they are ill suited. They do not have sufficient expertise or data, and there are too many disincentives to effectiveness. Dividing these tasks between the private sector and public financial intelligence units is inherently inefficient; not only does it separate data pools into many different private sector parties and the public sector, it reduces the overall role of the public sector in doing what it should do best: finding criminals and terrorists. It also makes the use of empirically based analytical tools like regression or discriminant function analysis both difficult (by dividing data bases) and unlikely (because the private sector has few incentives to spend the money to do so).

These problems can be addressed by turning all analytical work to public sector financial intelligence units and reserving for the private sector only the reporting of certain client profiling data and records of all financial transactions. Financial intelligence should be required to use, to the extent possible, empirical analysis, results should be far better than the current system. While such a system would be substantially different from the current one, there is considerable precedent in the way in which modern tax administrations select taxpayers for audit investigation. Also, there should be significant over-all cost savings as redundancies among
multiple private sector party analytical duties are eliminated. Both the private sector, which would experience significant cost reductions, and public sector civil servants, who would see an increase in duties and financial support, would be expected to support such changes. While these changes would entail a larger cost to the public fisc, because this would in part finance greater governmental anti-terrorism work the added public sector costs might be politically acceptable.