LOSING THE WAR AGAINST DIRTY MONEY: RETHINKING GLOBAL STANDARDS ON PREVENTING MONEY LAUNDERING AND TERRORISM FINANCING

RICHARD K. GORDON*

"We must now wage an all-out war to prevent money laundering and the financing of terrorism."[1]

"One and one is two.
Two and two is four.
I feel so bad
'Cause I'm losing the war."[2]

INTRODUCTION

Since at least the 1970s, there has been a sustained and increasingly global interest in stopping money laundering.[3] The reasons are hardly

* 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 2004 the author served as a senior staff member of the International Monetary Fund where he worked, among other things, on the development and implementation of global standards for the prevention of money laundering and terrorism financing. 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, David Chaikin, Graeme Cooper, Erik Jensen, Peter Gerhart, Willie Maddox, Richard Vann, Alvin Warren, Mira Kasliwal, and Emile van de Does de Willebois.

1. Jochen Sanio, President, Financial Action Task Force and President, Federal Banking Supervisory Office, Federal Republic of Germany, Washington D.C., August 8, 2002.

2. Mel Brooks, *The Producers* (1968).

3. For example, the first anti-money laundering law enacted in the U.S. was The Currency and Foreign Transactions Reporting Act of 1970 (Bank Secrecy Act) P.L. 91-508, Titles I and II (codified as amended at 12 U.S.C. §§ 1829b, 1951-59 (2000) and 31 U.S.C. §§ 5311-5330 (2000) [hereinafter Currency Reporting Act]). Anti-money laundering laws were expanded in 1986, 88, 92, 94, 96, 2001, and 2004. FinCEN, *History of Anti-money Laundering Laws*, http://www.fincen.gov/news_room/aml_history.html (FinCEN is the U.S. financial intelligence Unit). *See* Mariano-Florentino Cuellar, *Criminal Law: The Tenuous Relationship Between the Fight Against Money Laundering and the Disruption of Criminal Finance*, 93 J. CRIM. L. & CRIMINOLOGY 311, 336-64 (2003) [hereinafter Cuellar, *Criminal Law*]. The European Union's efforts began in 1991 with its first anti-money laundering Directive (Council Directive 91/308/EEC, 1991 O.J. (L 166) (EC)) and were expanded significantly with the second and third anti-money laundering Directives in 2001 (Council Directive 2001/97/EC, 2001 O.J. (L 344) (EC)) and 2004 (Council Directive 2005/60/EC, 2005 O.J. (L 309) (EC)). *See* Alan E. Sorcher, *Lost In Implementation: Financial Institutions Face Challenges Complying*

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.[4] The state may also be able to confiscate the ill-gotten gains.[5] Criminals, therefore, seek to disguise the illegal origins of the proceeds of crime and their ownership of the proceeds.[6] At least in theory, preventing

With Anti-Money Laundering Laws, 18 TRANSNAT'L LAW. 395, 408-10, 414 (2005) [hereinafter Sorcher, *Lost In Implementation*]. The first multilateral convention including anti-money laundering provisions came into force in 1988. United Nations Convention Against the Illicit Traffic in Narcotic Drugs and Psychotropic Substances, Dec. 20, 1988, 1582 U.N.T.S. 95, *available at* http://www.unodc.org/pdf/convention_1988_en.pdf [hereinafter Vienna Convention]. This was followed by conventions expanding anti-money laundering provisions. The Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime ETS No. 141 (entered into force 1993), *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/141.htm [hereinafter Strasbourg Convention]; United Nations Convention against Transnational Organized Crime, Sept. 29, 2003, 2225 U.N.T.S. 209, *available at* http://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf. The Financial Action Task Force published its first set of 40 Recommendations on money laundering in 1990. These original Recommendations were revised and expanded in 1996. FINANCIAL ACTION TASK FORCE FORTY RECOMMENDATIONS ON MONEY LAUNDERING 2 (June 28, 1996). A revised version was issued in 2003, *available at* http://www.fatf-gafi.org/document/28/0,3746,en_32250379_32236920_33658140_1_1_1_1,00.html [hereinafter FATF 40 Recommendations]. Following the attacks of September 11, 2001 the FATF added 8 Special Recommendations against Terrorism Finance; a 9th Recommendation was added in 2004. FATF, Terrorist Financing, *available at* http://www.fatf-gafi.org/pages/0,3417,en_32250379_32236947_1_1_1_1_1,00.html [hereinafter IX Special Recommendations].

4. Large amounts of cash can be bulky, hard to move, and draw the attention of law enforcement, Richard Gordon, *Trysts or Terrorists? Financial Institutions and the Search for Bad Guys,* 43 WAKE FOREST L. REV. 699, 708-09 (2008) [hereinafter Gordon, *Trysts or Terrorists*], while checks, credit cards, etc., can create a financial trail linking funds to the person(s) making the payment. ROGER C. MOLANDER, B. DAVID MUSSINGTON & PETER A. WILSON, CYBERPAYMENTS AND MONEY LAUNDERING (1998).

5. For a history of forfeiture laws in the U.S., see David J. Fried, *Criminal Law: Rationalizing Criminal Forfeiture*, 79 J. CRIM. L. & CRIMINOLOGY 328, 335-57 (1988) and Barclay Thomas Johnson, *Restoring Civility-the Civil Asset Forfeiture Reform Act of 2000: Baby Steps Towards a More Civilized Civil Forfeiture System*, 35 IND. L. REV. 1045, 1047-53, 1070-73 (2001). Vienna Convention, *supra* note 3, at Art. 5 (limited to the proceeds of narcotics trafficking), Strasbourg Convention, *supra* note 3, at Art. 2, Palermo Convention, *supra* note 3, at Art. 12, and the FATF 40 Recommendations on Money Laundering, *supra* note 3, at Recommendation 3, require the adoption of forfeiture laws for the proceeds of crime.

6. "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." FINANCIAL ACTION TASK FORCE, MONEY LAUNDERING FAQ, *available at* http://www.fatf-gafi.org/document/29/0,3343,en_32250379_32235720_33659613_1_1_1_1,00.html.

criminals from succeeding makes it harder for them to benefit from their crimes.[7]

Over the past forty years anti-money laundering rules have been expanded, refined a bit, but rarely completely re-thought or substantially rewritten.[8] The vast majority of the world's jurisdictions now endorse the latest version of the Financial Action Task Force's Forty Recommendations on Money Laundering ("FATF 40 Recommendations")[9] and accompanying Methodology for Assessment.[10] Starting in 1990, these global standards

---

7. "[T]argeting 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." *Id*.

8. 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, *supra* note 3. 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, *supra* note 3. 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), *supra* note 3, at Recommendations 11-15; FATF 40 Recommendations (2003), *supra* note 3, at Recommendations 5-16.

9. According to the FATF 130 countries have endorsed the 40. FATF 40 Recommendations, *supra* note 3, 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, *available at* http://www.fatf-gafi.org/dataoecd/8/17/34849466.pdf). INTERNATIONAL MONETARY FUND, IMF ADVANCES EFFORTS TO COMBAT MONEY LAUNDERING AND TERRORIST FINANCE, Public Information Notice No. 02/87, August 8, 2002, *available at* 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 THE ANTI-MONEY LAUNDERING AND COMBATTING THE FINANCING OF TERRORISM (AML/CFT) STANDARD 1 (2002), *available at* 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, *available at* 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 as the global standard for anti- money laundering and combating the financing of terrorism. *See* FINANCIAL ACTION TASK FORCE, MEMBERS AND OBSERVERS, *available at* 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); s*ee also* PAUL ALLAN SCHOTT, REFERENCE GUIDE TO ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM III-7 – III-13 (2d ed. 2006), *available at* http://siteresources.worldbank.org/EXTAML/Resources/396511-1146581427871/Reference_Guide_AMLCFT_2ndSupplement.pdf [hereinafter SCHOTT, REFERENCE GUIDE].

10. FINANCIAL ACTION TASK FORCE, METHODOLOGY FOR ASSESSING COMPLIANCE WITH THE FATF 40 RECOMMENDATIONS AND FATF 9 SPECIAL RECOMMENDATIONS (2009), *available at* http://www.fatf-gafi.org/dataoecd/16/54/40339628.pdf [hereinafter Methodology].

have required financial institutions[11] to monitor the transactions of their customers and to report to special government authorities (known as financial intelligence units) those transactions they suspect might involve the proceeds of crime,[12] and since 2001, the financing of terrorism.[13] Financial intelligence units then analyze the reports along with other data and make recommendations to law enforcement as to which clients or transactions should be investigated.[14]

The terrorist attacks of September 11, 2001 greatly intensified the global "war" on money laundering and, for the first time, on terrorism financing.[15] In 2002, the International Monetary Fund and the World Bank adopted the FATF 40 Recommendations and the eight new Special Recommendations on Terrorism Financing as a world standard.[16] They, along with the Financial Action Task Force and various regional anti-money laundering groups, also began a joint global compliance program by assessing the extent to which individual countries were implementing those standards.[17] Failure to implement the standards adequately can result in a broad application of sanctions or countermeasures, including bans on doing business with financial institutions located within the borders of non-

11. INTERNATIONAL MONETARY FUND, REPORT ON THE OUTCOME OF THE FATF PLENARY MEETING AND PROPOSAL FOR THE ENDORSEMENT OF THE METHODOLOGY FOR ASSESSING COMPLIANCE WITH THE ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM (AML/CFT) STANDARD 1 (2002), *available at* http://www.imf.org/external/np/mae/aml/2002/eng/110802.pdf [hereinafter PROPOSAL FOR THE ENDORSEMENT OF THE METHODOLOGY].

12. FATF 40 Recommendations (1990) and FATF 40 Recommendations (1996), *supra* note 3, at Recommendations 11-15; FATF 40 Recommendations (2003), *supra* note 3, at Recommendations 5-16.

13. FATF Special Recommendations on Terrorist Financing (2001), *supra* note 9.

14. SCHOTT, REFERENCE GUIDE, *supra* note 9, at VII-3.

15. Richard K. Gordon, *On the Use and Abuse of Standards for Law: Global Governance and Offshore Centers*, 88 N.C. L. REV. 501, 564 (2010) [hereinafter Gordon, *On the Use and Abuse of Standards for Law*].

16. IMF ADVANCES EFFORTS TO COMBAT MONEY LAUNDERING AND TERRORIST FINANCE, Public Information Notice No. 02/87 (August 8, 2002), *available at* http://www.imf.org/external/np/sec/pn/2002/pn0287.htm.

17. A uniform system of assessment, including a single assessment methodology, was agreed to by the IMF, the World Bank, and the FATF in 2002. PROPOSAL FOR THE ENDORSEMENT OF THE METHODOLOGY, *supra* note 11, at 2. IMF assessment reports can be found at http://www.imf.org/external/ns/cs.aspx?id=175 and World Bank assessments at http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTFINANCIALSECTOR/EXTAML/0,,contentMDK:21995901~menuPK:396518~pagePK:148956~piPK:216618~theSitePK:396512,00.html. These bodies and each of the eight FATF associate members and FATF-style regional bodies (many of which are undertaken with the participation of the IMF and World Bank) use the uniform assessment system. FATF assessments can be found at http://www.fatf-gafi.org/pages/0,3417,en_32250379_32236963_1_1_1_1_1,00.html and those of regional bodies can be found at http://www.imf.org/external/np/leg/amlcft/eng/aml2.htm#reports.

complying jurisdictions.[18] As a result, millions of suspicious transaction reports have been forwarded to financial intelligence units by financial institutions throughout the world,[19] although how many have resulted in further investigation, prosecution, and conviction is not publically available.[20]

These measures to prevent money laundering and terrorism financing in the financial sector have been endorsed by nearly every country in the world.[21] The only major problem is that they do not seem to work.[22] In fact, this Article argues they *cannot* work, and that they 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[23] is wrong. Instead, the government should undertake the key role financial institutions currently play in deciding if their clients are possible money launderers or terrorists. The article also 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, this Article suggests, should be relegated to reporting only objective information on customers and transactions in much the way that

18. For example, under Title III, Sec. 311(a) of the U.S.A. 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, "[f]inancial 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."

19. Telephone Interview with Rick McDonnell, Staff Director, FATF, in Paris, Fr. (Feb. 28, 2010) [hereinafter McDonnell Interview]. In the U.S. alone, depository institutions filed over 4 million suspicious transaction reports between April 1996 and June 2009. The U.S. refers to suspicious transaction reports as suspicious activity reports or SARs. FinCEN, 13 SAR Review by the Numbers, Suspicious Activity Report FORM TD F-90-22.47, Suspicious Activity Report by Depository Institution, Exhibit 1: Suspicious Activity Report Filings by Year & Month, April 1, 1996 through June 30, 2009 (January 2010), *available at* http://www.fincen.gov/news_room/rp/files/sar_by_numb_13.pdf [hereinafter FinCEN SAR Reviews].

20. E-mail from Boudewijn Verhelst, President, Egmont Group of Financial Intelligence Units, to author (Feb. 27, 2010) [hereinafter Verhelst e-mail].

21. *See supra* note 9 and accompanying text.

22. This view has been expressed by many commentators, including governmental and private sector practitioners and academics. *See infra* notes 84-86 and accompanying text.

23. For purposes of this Article "private" includes state-owned financial institutions and others subject to preventive measures requirements. This is because state-owned persons are subject to most of the same constraints, incentives, and disincentives with respect to those requirements as are private, fully for-profit institutions.

certain third parties must report taxpayer transactions to revenue authorities.

Following a brief overview in Part I.A of the overall system to prevent money laundering, Part I.B describes the role of the private sector, 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.C continues the description of the preventive measures system by describing the government's role, 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.

Parts I.D and I.E examine the effectiveness of this system. Part I.D discusses successes and failures in the private sector's role. Borrowing from theory concerning the effectiveness of private sector unfunded mandates, this Part reviews why many aspects of the system are failing, focusing on the subjectivity of the mandate, the disincentives to comply, and the lack of comprehensive data on client identification and transactions. It notes that the system includes an inherent contradiction: the public sector is tasked with informing the private sector how best to detect launderers and terrorists, but to do so could act as a road map on how to avoid detection should such information fall into the wrong hands. Part I.D discusses how financial institutions do not and cannot use scientifically tested statistical means to determine if a particular client or set of transactions is more likely than others to indicate criminal activity. Part I.D then turns to a discussion of a few issues regarding the impact the system has but that are not related to effectiveness, followed by a summary and analysis of how flaws might be addressed.

Part I.E continues by discussing the successes and failures in the public sector's role. It reviews why the system is failing, focusing on the lack of assistance to the private sector in and the lack of necessary data on client identification and transactions. It also discusses how financial intelligence units, like financial institutions, do not and cannot use scientifically tested statistical means to determine probabilities of criminal activity. Part I concludes with a summary and analysis tying both private and public roles together.

Part II then turns to a review of certain current techniques for selecting income tax returns for audit. After an overview of the system, Part II first discusses the limited role of the private sector in providing tax administrators with information, comparing this to the far greater role the

private sector plays in implementing preventive measures. Next, this Part turns to consider how tax administrators, particularly the U.S. Internal Revenue Service, select taxpayers for audit, comparing this to the role of both the private and public sectors in implementing preventive measures. It focuses on how some tax administrations use scientifically tested statistical means to determine probabilities of tax evasion. Part II then suggests how flaws in both private and public roles of implementing money laundering and terrorism financing preventive measures might be theoretically addressed by borrowing from the experience of tax administration. 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. It suggests that financial intelligence units should be uniquely tasked with analyzing and selecting clients and transactions for further investigation for money laundering and terrorism financing. The private sector's role should be restricted to identifying customers, creating an initial profile of their legitimate activities, and reporting such information and all client transactions to financial intelligence units.

I. CURRENT STANDARDS FOR PREVENTING MONEY LAUNDERING AND TERRORISM FINANCING IN THE FINANCIAL SECTOR

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."[24] Together they cover, among other things, 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 other institutions subject to preventive measures, financial intelligence units, and international cooperation.[25] The 40 Recommendations have included

24. FATF 40 Recommendations (2003), *supra* note 3, at *Introduction*.

25. The FATF 40 Recommendations are broken down into four 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

similar preventive measure requirements since the original 1990 draft.[26] In effect, these Recommendations divide the responsibility for preventing and uncovering money laundering between the private and public sector.

B. Private Sector Role

FATF Recommendations 5 through 13 plus 21 and 22 (and the 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. Unfortunately these Recommendations are not a model of clarity and are not easy for non-experts to comprehend.[27] However, they are designed to create a five-part requirement:[28] (1)

---

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 34); 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, *supra* note 3.

26. Since 1990 there has been a progressive expansion of those persons who must follow the "preventive measures" provisions in the FATF 40 Recommendations. FATF Recommendations (1990), *supra* note 3 at Recommendation 5, FATF Recommendations (1996), *supra* note 3 at Recommendation 5. The current definition of financial institutions includes include any person who engages in acceptance of deposits and other repayable funds from the public; lending; financial leasing; the transfer of money or value; issuing and managing means 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 10, 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.

27. In 2002 an attempt was made by the International Monetary Fund to reorganize the preventive measures Recommendations into a more accessible, coherent whole. However, in a series of meetings in 2002 delegations to the FATF rejected the effort.

28. 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

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;[29] (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.[30] Recommendations 18, 19, and 26 through 34 (and the 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.

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 and terrorist elements. It does this by making financial institutions and other institutions subject to preventive measures identify and profile potential (and, periodically, existing) customers to screen out possible criminals and terrorists.[31] 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 their transactions.[32] 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

money laundering and the financing of terrorism as part of a model law on antimony laundering and terrorism financing. The Model Regulation implements these FATF Recommendations based on the regulatory frameworks in the U.K., 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.*

29. 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.*

30. *See infra* notes 52–55 and accompanying text.

31. *See infra* notes 38–48 and accompanying text.

32. *See infra* notes 49–51 and accompanying text.

enforcement those that raise suspicion that criminal proceeds or terrorism financing are involved.[33]

The United States largely 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 issued to financial institutions.[34] The European Union also largely complies through both Directives (essentially instructions to members of the Union) and implementing legislation at the member country level.[35] The language used to implement the Recommendations is often similar to that found in the Recommendations.[36]

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.[37]

1. Customer Identification, Customer Profiling, Record-Keeping

FATF Recommendation 5 requires that financial institutions 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

33. *See infra* notes 52–64 and accompanying text.

34. FINANCIAL ACTION TASK FORCE, THIRD MUTUAL EVALUATION REPORT ON ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM, UNITED STATES OF AMERICA 83-197 (financial institutions), 198–226 (designated non-financial businesses and persons) (2006), *available at* http://www.fatf-gafi.org/dataoecd/44/9/37101772.pdf [hereinafter U.S. MUTUAL EVALUATION REPORT]. *See also* M. MAUREEN MURPHY, CRS REPORT FOR CONGRESS: INTERNATIONAL MONEY LAUNDERING ABATEMENT AND ANTI-TERRORISM FINANCING ACT OF 2001, *available at* http://epic.org/privacy/financial/RL31208.pdf; Megan Roberts, *Big Brother Isn't Just Watching You, He's Also Wasting Your Tax Payer Dollars: An Analysis of the Anti-Money Laundering Provisions of the USA Patriot Act,* 56 RUTGERS L. REV. 573, 586 (2004). Regulations on customer identification are found in 31 C.F.R. § 103.121. 31 U.S.C. § 5314(b) (2006) authorizes the Secretary of the Treasury to require financial institutions to report suspicious transactions. It is implemented at 21 C.F.R. § 21.110. There are similar customer identification rules for securities broker-dealers, mutual funds, and futures commission merchants and introducing brokers in commodities. Financial Recordkeeping and Reporting of Currenct and Foreign Transactions, 31 CFR § 103.122, 131 (2006); ASD, NOTICE TO MEMBERS 02-21 5–7 (2002); NASD, NOTICE TO MEMBERS 03-34 (2003). Under 31 CFR § 103.137(c), a life insurer is required to have policies and procedures for obtaining "all relevant customer-related information necessary for an effective anti-money laundering program."

35. Sorcher, *Lost in Implementation*, *supra* note 3, at 408–10.

36. In the course of his assessment work for the International Monetary Fund and the World Bank the author of this Article has reviewed implementing statutory and regulatory language in The British Virgin Islands, Hong Kong, Niger, the Philippines, Rwanda, Sierra Leone, and the United Kingdom and often found language nearly identical to that used in the Recommendations and Methodology. This may be due to decisions to enact the two verbatim so as to ensure that legislation complies with the standard.

37. *See infra* Part I.D.

persons who own or control the legal person.[38] Recommendation 12 extends these requirements to certain designated non-financial businesses and persons, which include casinos (which often deal with cash that can be exchanged for chips and visa versa, providing laundering opportunities), 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, plus the fact that the ownership of precious metals can be easily transferred), lawyers, notaries, and persons who assist in the setting up of trusts and companies (these are often professionals who assist launderers in hiding assets). For simplicity this Article will refer to those private sector persons subject to preventive measures requirements as "financial institutions and Designated NonFinancial Businesses and Professions ("DNFBP")."[39] Although neither the Recommendation itself nor the Methodology uses the term "client profile," Recommendation 5 requires that the financial institution and DNFBP "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."[40]

This serves two purposes. If a potential client's identity and profile cannot be established, the financial institution and certain others must terminate the business relationship.[41] Second, future transactions of accepted clients can be measured against this baseline of normal or typical transactions. Specifically, financial institutions and DNFBP must "understand the purpose, intended relationship, and conduct with the customer, 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."[42] In the event the financial institution and DNFBP cannot comply, the financial institution should terminate business relations or not undertake a

38. FATF 40 Recommendations (2003), *supra* note 3, at Recommendation 5. The Methodology allows an exception from this latter requirement in the event the legal person is a public company. Methodology, *supra* note 10, at Criterion 5.5.2(b).

39. FATF 40 Recommendations (2003), *supra* note 3, at Recommendation 12. Recommendation 22 requires that the principles applicable to financial institutions also be applied to branches and majority owned subsidiaries located abroad. *Id.* at Recommendation 22.

40. *Id.* at Recommendation 5.

41. Recommendation 18 also forbids financial institutions to transact business with shell banks and "guard against" establishing relations with those that do. *Id.* at Recommendation 18.

42. *Id.* at Recommendation 5.

transaction.[43] Second, the client profile allows the financial institution and DNFBP 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.[44] According to the Financial Action Task Force the adoption of risk sensitivity "involve[s] identifying and categorizing money laundering risks and establishing reasonable controls based on risks identified . . . ."[45] 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.[46] FATF Recommendation 5 now allows financial institutions and DNFBP to determine the extent of such measures on a risk-sensitive basis, depending on the type of customer, business relationship, or transaction.[47] Other Recommendations address new technologies and reliance on third parties for due diligence.[48]

---

43. It should also be made mandatory to file a suspicious transaction report to the Financial Intelligence Unit, but is not required to do so. *Id*. at Recommendation 13.

44. 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.

45. FATF, GUIDANCE ON THE RISK-BASED APPROACH TO COMBATING MONEY LAUNDERING AND TERRORIST FINANCING: HIGH LEVEL PRINCIPLES AND PROCEDURES 1–2 (2007), *available at* http://www.fatf-gafi.org/dataoecd/43/46/38960576.pdf [hereinafter FATF, GUIDANCE ON THE RISK-BASED APPROACH]. The United States has adopted a risk-based system. FFIEC, Bank Secrecy Act / Anti-Money Laundering Examination Manual 11–27, I-1, K-1, M-1, M-2 (2006) [hereinafter FFIEC MANUAL].

46. FATF 40 Recommendations, *supra* note 3. According to the FATF, the new focus on risk allows financial institution and DNFBP and supervisory authorities to be more efficient and effective in their use of resources and minimize burdens on customers, although it does not say exactly how. GUIDANCE ON THE RISK-BASED APPROACH, *supra* note 45, at 2. During the years when the FATF was considering the adoption of a risk based-approach disagreement tended to arise at between those FATF delegates from a law enforcement background and those from a regulatory, particularly bank regulatory background, with the latter arguing in favor of a risk-based approach. In general, the banking regulators were used to dealing with concepts of risk while law enforcement was not. "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.

47. FATF 40 Recommendations, *supra* note 3, at Recommendation 5. The Methodology goes on to provide certain examples of higher risk categories. Methodology, *supra* note 10, at Criteria 5.8 and 5.9. 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." FATF 40 Recommendations, *supra* note 3, at Recommendation 6. It requires financial institutions and DNFBP to have risk management systems to determine if customers are politically-exposed persons and to take reasonable measures to

Recommendation 10 requires that financial institutions and DNFBP 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[49] (Special Recommendation VII provides more detail with respect to wire transfers).[50] This, along with Recommendation 5, allows investigative and prosecutorial authorities to "follow the money" of criminal suspects.[51]

2. Transaction Monitoring and Suspicious Transaction Reporting

Recommendation 11 requires that financial institutions and DNFBP pay special attention to "complex, unusual large transactions, and 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.[52] This requirement is separate from Recommendation 5's requirement for ongoing customer due diligence with respect to "scrutiny of transactions."[53] Recommendation 13 requires that a financial institution and DNFBP 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. The

---

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 certain others must always take measures to establish the source of funds. Recommendation 6 was added in 2003 to address a perceived public backlash against developed country banks that had laundered the proceeds of developed country dictators. *Id.*

48. Under FATF Recommendation 8, financial institutions "should pay special attention to any money laundering threats that may arise from new or developing technologies" and must have "policies and procedures in place" to address any specific risks associated with non-face to face business relationships or transactions. *Id*. at Recommendation 8. FATF Recommendation 9 permits financial institutions to rely on third parties to undertake some due diligence measures in certain cases. *Id*. at Recommendation 9.

49. FATF Recommendation 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." *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, *supra* note 10, at page 62.

50. IX Special Recommendations, *supra* note 3, at Special Recommendation VII.

51. The United States has put in place similar rules. FFIEC MANUAL, *supra* note 45, at 21, 118–22, 261–64.

52. FATF 40 Recommendations, *supra* note 3, at Recommendation 11.

53. *Id.* at Recommendation 5.

Methodology describes this as filing a suspicious transaction report.[54] Special Recommendation IV further requires financial institutions and DNFBP to file reports if they suspect terrorism financing.[55] It is these Recommendations, along with Recommendation 5, that create the system requiring financial institution and DNFBP to monitor customer transactions based on their profiles and to report to law enforcement those that raise suspicion that criminal proceeds or terrorism financing might be involved. Recommendation 15 requires financial institutions to develop internal policies, procedures, and controls for anti-money laundering programs, including compliance management arrangements, internal training, and audit capacities.[56] Recommendation 16 extends most of these requirements to the same DNFBP as found in Recommendation 12, although not all.[57]

An essential aspect of this part of the preventive measures system should be emphasized. Financial institutions and DNFBP must design and implement their own systems.[58] While the five-part requirement describes

54. *Id* .at Recommendation 13.

55. IX Special Recommendations, *supra* note 3, at Special Recommendation IV. Recommendation 21 requires that financial institutions and DNFBP pay "special attention" to business relationships and transactions with persons from countries that do not or insufficiently apply the FATF Recommendations (although it does not say how this is to differ from non-special (average?) attention). FATF 40 Recommendations, *supra* note 3, at Recommendation 21. This Recommendation raises the costs of doing business with persons from countries that do not sufficiently apply the Recommendations as a whole. This creates a financial incentive for countries to implement the Recommendations, especially as determined by assessment reports.

56. FATF 40 Recommendations, *supra* note 3, at Recommendation 15.

57. *Id.* at Recommendation 16. Recommendation 14 protects financial institution and DNFBP from any liability for filing suspicious activities reports and prohibits the reporting person from revealing that such reports are being made (known as the prohibition against tipping off). U.S. rules comply with these requirements, except that DNFBP include casinos only. 31 CFR § 103.18,19 (2006).

58. *See, e.g.*, FATF 40 Recommendations, *supra* note 3, at Recommendation 5 ("Financial institutions *should undertake* customer due diligence measures . . . but *may determine the extent* of such measures on a risk sensitive basis . . . .") (emphasis added); *Id.* at Recommendation 6 (Financial systems *should "[h]ave appropriate risk management systems*") (emphasis added); *Id.* at Recommendation 8 ("Financial institutions *should have policies and procedures in place* to address any specific risks associated with nonface to face business relationships or transactions.") (emphasis added); *Id.* at 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") (emphasis added); *Id.* at Recommendation 10 ("[R]ecords *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.") (emphasis added); *Id.* at Recommendation 11 ("Financial institutions *should pay special attention* to all complex, unusual large transactions . . . . The 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.") (emphasis added); *Id.* at Recommendation 13("If 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. . . .") (emphasis added); *Id.* at Recommendation 15 ("Financial institutions *should develop program[]s* against money

what these systems are supposed to accomplish, it does not provide any detail as to how they are supposed to do it. Financial institutions and DNFBP are not told how to 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."[59] Both how governmental agencies provide guidelines and feedback, and how the private sector implements its preventive measure requirements, are discussed below.

C. Public Sector Role

1. Overview

Recommendations 18, 19, and 26 through 32 (and the relevant materials in the accompanying Methodology for assessment of compliance) address both the supervisory system to ensure private sector compliance with its preventive measures requirements and the criminal investigation and prosecution system for state law enforcement authorities.[60] As shall be seen, the public sector's role focuses on three basic objectives. The first is to ensure the private sector's compliance with their preventive measure responsibilities.[61] Essentially, governmental authorities must supervise and regulate financial institutions and DNFBP to ensure compliance. This must include both guidance and examination functions, including the potential application of sanctions. The second is to ensure that suspicious transaction reports lead to the investigation of appropriate cases of suspected crime and terrorism.[62] Essentially, a financial intelligence unit receives and analyzes these reports along with other key information. It then decides which should be further investigated[63] and forwards these to the appropriate government agency (typically the police). They then, sometimes in consultation with state prosecutors, decide whether and how to go forward.[64]

---

laundering and terrorist financing . . . [including] *[t]he development of internal policies, procedures and controls, including appropriate compliance management arrangements* . . . .") (emphasis added).

59. *Id.* at Recommendation 25.

60. 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." *See* FATF 40 Recommendations, *supra* note 3.

61. *See infra* notes 79–83 and accompanying text.

62. *See infra* notes 86–89 and accompanying text.

63. *See infra* notes 86–89 and accompanying text.

64. *See infra* notes 214–215 and accompanying text.

2. Guidelines, Feedback, and Supervision

Recommendation 25 requires that government authorities establish guidelines and provide feedback to assist financial institutions and DNFBP, in particular "in detecting and reporting suspicious transactions."[65] 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 are implemented by financial institutions and DNFBP.[66] This includes information on current techniques, methods and trends (typologies), [67] 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.[68]

In order to ensure compliance with the preventive measures, Recommendation 23 requires that financial institutions and DNFBP be subject to adequate regulation and supervision to ensure implementation of the preventive measures,[69] while Recommendations 29 and 17 require that supervisors have adequate powers to ensure compliance including the imposition of sanctions.[70]

---

65. FATF 40 Recommendations, *supra* note 3 at Recommendation 25.

66. Methodology, *supra* note 10, at criteria 25.1–2.

67. "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, *available at* http://www.fatf-gafi.org/pages/0,3417,en_32250379_32237202_1_1_1_1_1,00.html.

68. *See supra* notes *47*, 58, and accompanying text.

69. FATF 40 Recommendations, *supra* note 3, at Recommendation 23. Recommendation 24 extends this requirement to designated non-financial businesses and persons. *Id.* at Recommendation 24.

70. *Id.* at Recommendations 29, 17. U.S. laws also comply with these requirements. 31 C.F.R. § 103 (2004), 17 C.F.R. § 240.17a, 1.32–37 (1948). The U.S. has levied significant fines, as well as other supervisory and regulatory orders, against financial institutions and casinos. "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." David Zaring & Elena Baylis, *Sending the Bureaucracy to War*, 92 IOWA L. REV. 1361, 1414–15 (2007) (citations omitted) [hereinafter Zaring & Baylis, *Bureaucracy to War*].

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[71] that serves as a national center 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.[72] Recommendation 10 states that competent authorities (including financial intelligence units) should have access to records kept by financial institutions and DNFBP.[73] Finally, Recommendation 40 states that countries should ensure that their competent authorities provide the widest possible range of international co-operation to their foreign counterparts, including information relating to money laundering, provided 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.[74] 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, subject to confidentiality safeguards limiting the

71. 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: AN OVERVIEW 56 (2004), *available at* http://www.imf.org/external/pubs/ft/fiu/fiu.pdf [hereinafter IMF, FINANCIAL INTELLIGENCE UNITS]. This Article refers to the financial intelligence unit using a functional definition.

72. FATF 40 Recommendations, *supra* note 3, at Recommendation 26. For example, FinCEN has access to numerous databases. 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 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/CBFTFS_Complete.pdf [hereinafter FINCEN, CROSS-BORDER ELECTRONIC FUNDS].

73. FATF 40 Recommendations, *supra* note 3, at Recommendation 10.

74. *Id.* at Recommendation 40.

use of the data.[75] This is the only substantive Recommendation relating to financial intelligence units (the Methodology adds little).[76]

A few other key recommendations relate to the implementation of preventive measures. Potentially the most important are 33 and 34. Recommendation 33 requires that countries ensure that timely information on the beneficial ownership and control of legal persons is available and 34 extends this requirement to "express trusts" and other trust-like legal relationships.[77] These Recommendations relate to the customer identification requirements of Recommendation 5. However, Recommendations 33 and 34 are highly problematic in common law countries where information on beneficial ownership or trust relations is not kept by government agencies.[78] 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." The Recommendation goes on to state that "non-profit organisations are particularly vulnerable, and countries should ensure that they cannot be misused . . . by terrorist organisations posing as legitimate entities."[79]

D. Private Sector Successes and Failures

1. Overview

There are a number of public policy considerations relating to the privatization of preventive measures. The most important is the effectiveness of implementation, followed by cost and certain data access

75. Methodology, *supra* note 10, at Criterion 40.4.1.

76. 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* note 153 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. The U.S. largely complies with these requirements. U.S. MUTUAL EVALUATION REPORT, *supra* note 34, at 226-40.

77. FATF 40 Recommendations, *supra* note 3, at Recommendations 33 and 34.

78. U.S. MUTUAL EVALUATION REPORT, *supra* note 34, at 226-40.

79. IX Special Recommendations, *supra* note 3, at Recommendation VIII. Recommendation 18 forbids the licensing of shell banks, or banks that have no physical presence and that are therefore easy to set up and difficult to regulate. FATF 40 Special Recommendations (2003), *supra* note 3 at Recommendation 18.

issues. Compliance assessments have generally found that record-keeping requirements have been effectively implemented.[80] This is less true of the customer identification[81] and profiling requirements, where implementing rules have sometimes been found to be inadequate or where effectiveness has been difficult to determine, especially with respect to beneficial ownership. [82] Concerns as to the workability of these requirements can be

80. Verhelst e-mail, *supra* note 20. This is demonstrated by the fact that no FATF papers have been commissioned or written concerning failures in the record-keeping requirements. Also, a review of several recent assessment reports indicates no problems with recordkeeping. *See, e.g.*, U.S. MUTUAL EVALUATION REPORT, *supra* note 34, at 126–36; FATF, MUTUAL EVALUATION REPORT: ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM AUSTRIA 127-30 (2009), *available at* http://www.fatf-gafi.org/dataoecd/22/50/44146250.pdf [hereinafter AUSTRIA MUTUAL EVALUATION REPORT]; FATF, THIRD MUTUAL EVALUATION REPORT: ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM, AUSTRALIA 80–84 (2005), *available at* http://www.fatf-gafi.org/dataoecd/60/33/35528955.pdf [hereinafter AUSTRALIA MUTUAL EVALUATION REPORT]; FATF, THIRD MUTUAL EVALUATION REPORT: ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM, CANADA 149–154 (2008), *available at* http://www.fatf-gafi.org/dataoecd/5/3/40323928.pdf [hereinafter CANADA MUTUAL EVALUATION REPORT]; FATF, THIRD MUTUAL EVALUATION REPORT: ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM, UNITED KINGDOM 132–39 (2007), *available at* http://www.fatf-gafi.org/dataoecd/55/29/39064399.pdf [hereinafter U.K. MUTUAL EVALUATION REPORT]*;* FATF, THIRD MUTUAL EVALUATION REPORT: ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM, HONG KONG, CHINA 104–11 (2008), *available at* http://www.fatf-gafi.org/dataoecd/19/38/41032809.pdf [hereinafter HONG KONG CHINA MUTUAL EVALUATION REPORT].

81. Verhelst e-mail, *supra* note 20. 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 34 (not discussed at all); AUSTRIA MUTUAL EVALUATION REPORT, *supra* note 80, at 102-103, 105 (not discussed in detail); AUSTRALIA MUTUAL EVALUATION REPORT, *supra* note 80, at 70 (inadequate rules obviate discussion of their effectiveness); CANADA MUTUAL EVALUATION REPORT, *supra* note 80, at 129 (inadequate rules obviate discussion of their effectiveness); U.K. MUTUAL EVALUATION REPORT, *supra* note 80, 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 *supra* note 80 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.

82. Verhelst e-mail, *supra* note 20. The overall effectiveness of client profiling tends not to be addressed in FATF compliance reports (or only briefly with little information), often because the rules implementing the FATF Recommendations are inadequate. *See, e.g.*, U.S. MUTUAL EVALUATION REPORT, *supra* note 34 (not discussed at all) ; AUSTRIA MUTUAL EVALUATION REPORT, *supra* note 80, at 106 (not discussed); AUSTRALIA MUTUAL EVALUATION REPORT, *supra* note 80, at 71 (inadequate rules obviate discussion of their effectiveness); CANADA MUTUAL EVALUATION REPORT, *supra* note 80, at 130 (inadequate rules obviate discussion of their effectiveness); U.K. MUTUAL EVALUATION REPORT, *supra* note 80, at 116 (inadequate rules obviate discussion of their effectiveness); HONG KONG CHINA MUTUAL EVALUATION REPORT, *supra* note 80, 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.

based both on the effectiveness of the system as designed by the FATF Recommendations[83] and on how that system is implemented.

According to some scholars there is little evidence that preventive measures have reduced money laundering.[84] This is particularly true with respect to transaction monitoring and suspicious transaction reporting requirements, where both scholars and practitioners have raised serious doubts as to whether they actually work to help catch money launderers and terrorist financers.[85] For example, in the U.S., suspicious transaction reports have apparently led to very few investigations; in fact, FinCEN, the U.S. financial intelligence unit, does not even report how many are reviewed by government authorities.[86] Statistics collected in the course of Financial Action Task Force mutual evaluations of other countries also suggest that few successful investigations are developed from suspicious transaction reports.[87] If reporting helps it may only be at the ex post stage, when the authorities can use records to follow the money, not at the detection or "preventive" stage. There is also a strong indication that many financial institutions do not believe that financial intelligence units or other governmental authorities make much use of suspicious activity reports, in part because the reports are too numerous to be helpful.[88] Perhaps most significantly, a common, if more private, refrain by financial intelligence unit and financial investigator experts at FATF is that the system of client profiling and monitoring of transactions simply does not work to provide a

---

83. 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* note 85 and accompanying text.

84. Investigations have a failure rate of 99.9%. Zaring & Baylis, *Bureaucracy to War*, *supra* note 70, at 1413.

85. FATF mutual evaluation reports usually consider only the efficiency of the system as required under the Recommendations and not overall effectiveness at actually preventing money laundering or terrorism financing. Rules implementing the FATF Recommendations are themselves often found to be inadequate. *See, e.g.*, U.S. MUTUAL EVALUATION REPORT, *supra* note 34, at 160; AUSTRIA MUTUAL EVALUATION REPORT, *supra* note 80, at 106; AUSTRALIA MUTUAL EVALUATION REPORT, *supra* note 80, at 71; CANADA MUTUAL EVALUATION REPORT, *supra* note 80, at 130; U.K. MUTUAL EVALUATION REPORT, *supra* note 80, at 116; HONG KONG CHINA MUTUAL EVALUATION REPORT, *supra* note 80, at 97. With respect to technical issues in implementation *see infra* notes 239-241 and accompanying text.

86. Cuellar, *Criminal Law*, *supra* note 3 at 323, 378.

87. *See, e.g.*, AUSTRIA MUTUAL EVALUATION REPORT, *supra* note 80, at 132; AUSTRALIA MUTUAL EVALUATION REPORT, *supra* note 80, at 112-14; CANADA MUTUAL EVALUATION REPORT, *supra* note 80, at 213-14; U.K. MUTUAL EVALUATION REPORT, *supra* note 80, at 178; HONG KONG CHINA MUTUAL EVALUATION REPORT, *supra* note 80, at 96-98.

88. "Frustration mounts that . . . [the suspicious transaction reports] filed were of no use to apathetic or overwhelmed government authorities." John Adams, *Anti-Money Laundering: Diligence is Getting Pretty Pricey*, Bank Technology News (August 2007), *available at* http://www.dominion-advisors.com/press/in-the-news/2007/anti-money-laundering-diligence-getting-pretty-pricey [hereinafter Adams, *Diligence is Getting Pretty Pricey*].

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 how policy is effectively implemented though a particular law or rule.[89] They identify three broad categories that determine whether a person (actor) subject to a legislative mandate will effectively implement that mandate: the actor's understanding of the relevant rule (objective knowledge); the actor's anticipation of the implementing agency's behavior (the government's incentive or disincentive effects as applied to the actor); and the non-legal constraints and resources of the actor's own environment.[90] They further divide these three broad categories into seven sub-categories: (1) the precise wording of the rule; (2) the actor's opportunity to obey the rule (3) the actor's capacity to obey the rule, (4) the communication of the rule to the actor, (5) the actor's incentive to obey or disobey the rule, (6) the process by which the actor decides 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 finally (7) the actor's ideology.[91]

One can further consolidate and elucidate these categories so that they are clear and easy to apply in the case of preventive measures. First, the more clearly stated[92] and objective[93] a rule is, the easier it is for both the

89. *See generally* ANN SEIDMAN, ROBERT B. SEIDMAN & NALIN ABEYSEKERE, LEGISLATIVE DRAFTING FOR DEMOCRATIC SOCIAL CHANGE (2001) [hereinafter SEIDMAN *ET AL.* LEGISLATIVE DRAFTING].

90. *Id.* at 94.

91. *Id.* at 95-6. *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?*].

92. *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 DESK BOOK 169-240 (2006) (describing the importance of writing effectively in legislative drafting and emphasizing that "the essence of effective drafting is clear writing"), citied in Seidman *et al.*, *Is Legislation an Unprinciples Mess?*, *supra* note 91, 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.

93. Meaning a standard relatively less subject to interpretation (as in "clear and objective standards" that provide "specific and detailed guidance"), *Godfrey v. Georgia*, 446 U.S. 420, 428 (1980), quoted in Carol S. Steiker and Jordan M. Steiker, *Sober Second Thoughts: Reflections on Two Decades of Constitutional Regulation of Capital Punishment*, 109 HARV. L. REV. 355, 379–80 (1995), is not objective as in revealing a particular truth. *See* Edward L. Rubin, *Social Movements and Law*

actor and the enforcing authority to implement. Effective input and feedback by the implementing authority is a part of this communication, in that it helps the actor to correct her or his understanding of the rule. Second, the process by which the actor decides whether and how to obey the rule is affected by incentives, including economic or other incentives and any sanctions (or benefits) applied by the implementing authority. Third, the actor's capacity to obey the rule may be limited, meaning she or he may simply not have the means to do so. Finally, the actor may have an ideological reason favoring or disfavoring implementation, which would affect her or his motivation.

With respect to the effectiveness of implementation by financial institutions and DNFBP of the Financial Action Task Force's preventive measures, three effects appear to dominate: (1) the clarity and objectivity of the standard as supplemented by feedback from implementing agencies, (2) economic incentives plus the effect of sanctions for non-compliance, and (3) objective capacity. This Article will now address these three basic effects.

2. Clarity and Objectivity of the Rule

As noted earlier, compliance assessments have generally found that record-keeping requirements have been effectively implemented.[94] This should not be too surprising in that 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 certain should go in doing so.[95] In other words, they are highly subjective. The Recommendations state that financial institutions and DNFBP must take "reasonable measures" to verify the identity of the beneficial owner of an account such that the financial institution or DNFBP "is satisfied" that it knows who the beneficial owner is.[96] This includes taking "reasonable measures" to understand the ownership and control

Reform: Passing Through the Door: Social Movement Literature and Legal Scholarship, 150 U. PA. L. REV. 1, 34–46 (2001) (discussing critical theory and objectivity).

94. *See supra* note 79 and accompanying text.

95. *See supra* notes 80–84 and accompanying text.

96. *See supra* note 38 and accompanying text.

structure of the customer.[97] "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.[98] 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.[99] Recommendation 11 requires that "special attention" be paid to transactions that have no "apparent" economic or visible lawful purpose, and that their background and purpose be examined "as far as possible."[100] Recommendation 13 requires the reporting of transactions that a financial institution or DNFBP "suspects or has reasonable grounds to suspect" are the proceeds of a criminal activity or are related to terrorist financing.[101] Finally, Recommendation 15 requires "appropriate" compliance management arrangements.[102]

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, unavoidably giving rise to subjective implementation.[103] For example, would a "reasonable measure" to verify the identity of the beneficial owner be simply asking the client if there was a beneficial owner other than the person opening the account, or should a bank hire a private investigator? What constitutes "special attention" to transactions which have no "apparent" economic or visible lawful purpose? Should a bank simply give a once-over review based on the examiner's past experience or should it investigate each of the client's activities in detail?

The use of such highly subjective terms does, however, make clear that financial institutions and DNFBP must *design* as well as implement their own systems based on considerable subjective judgment. An important aspect of this "design and implement" requirement is the new risk-based option. Because client identification and profiling measures

97. *Id.*

98. FATF 40 Recommendations, *supra* note 3, at Recommendation 5.

99. *Id.* at Recommendation 6.

100. *Id.* at Recommendation 11.

101. *Id.* at Recommendation 13.

102. *Id.* at Recommendation 15.

103. Not surprisingly the lack of clarity in the rules as transferred to legislation is a major complaint of the private sector. KPMG INTERNATIONAL, GLOBAL ANTI–MONEY LAUNDERING SURVEY 2007: HOW BANKS ARE FACING UP TO THE CHALLENGE 7-8 (2007), *available at* http://us.kpmg.com/microsite/FSLibraryDotCom/docs/AML2007FULL.pdf [hereinafter KPMG, ANTI–MONEY LAUNDERING SURVEY].

may be applied on a risk sensitive basis as is "determine[d]" by the financial institution or DNFBP,[104] such persons 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 treatmen*t, and lack of understanding by customers . . ."[105] On their face these rules add even more subjectivity and discretion.

There is another problem that is not directly related to the lack of clarity and subjective nature of the Recommendations. While the client identification and profiling requirements include a risk component, [106] the monitoring and reporting requirements do not.

Suspicious transactions will have different degrees of likelihood that criminal proceeds or terrorism financing are involved. In theory, a transaction could be ranked from a near zero risk that it includes crime proceeds or finances terrorism, up to a near certainty that it does. However, the Recommendations do not state at which point a financial institution or DNFBP should report, or if it should even make a notation of estimated risk on the suspicious transaction report. This makes a real "risk sensitive" system difficult if not impossible to apply.

Next, suspicious transactions will vary as to the size or amount of criminal proceeds or terrorism financing, from a single penny to billions. However, the preventive measures standards do not provide guidance as to whether financial institutions and DNFBP should consider all transactions equally, regardless of the size of the suspected criminal proceeds, or whether they should focus on transactions with relatively large amounts of suspected criminal proceeds. While it might appear logical for financial institutions to apply greater efforts to determine the probity of relatively larger transactions, there is no guidance to this effect.

One restriction on the discretion afforded by the Recommendations and Methodology could come from the methods, trends, typologies, and feedback that government authorities are required to provide financial institutions and DNFBP.[107] Methods, trends, and typologies are produced

104. *See supra* notes 44-47 and accompanying text.

105. FATF, GUIDANCE ON THE RISK-BASED APPROACH, *supra* note 45, at 2 (emphasis added).

106. *See supra* notes 44-47 and accompanying text.

107. *See supra* notes 65-68 and accompanying text.

and published by the Financial Action Task Force, FATF associate members, FATF-style regional bodies,[108] and national authorities, especially financial intelligence units. However, such guidance and feedback rarely include assistance in interpreting terms or designing systems for profiling, monitoring, and reporting. Rather, they normally only provide examples of activities that heighten the risk that a particular client or transaction represents the proceeds of crime or terrorism financing. These tend to be limited to basic examples, such as which geographical areas include a higher incidence of terrorism (e.g. Pakistan) or typical tactics used by launderers (e.g. transfers among different shell companies).[109] They do not include examples of effective *systems* to detect them.

For example, FinCEN, the U.S. financial intelligence unit, provides many sanitized examples (meaning that identifying information like actual names and dates are deleted) of past cases of laundering and terrorism.[110] It also provides what it refers to as "red flags" that indicate a higher risk of laundering and terrorism finance, which are also based on prior cases.[111] Such "red flags" include, for example, "[a] customer uses unusual or suspicious identification documents that cannot be readily verified" or "[t]he customer's background differs from that which would be expected on the basis of his or her business activities."[112] Besides being rather obvious, these "red flags" do not tell the financial institution or DNFBP what kind of diligence to apply to these transactions or at what point they should report them. Oddly, FinCEN does not even make objective information readily

108. *See supra* note 67.

109. *See, e.g.*, FATF-GAFI, MONEY LAUNDERING METHODS & TRENDS, *available at* http://www.oecd.org/pages/0,3417,en_32250379_32237277_1_1_1_1_1,00.html; FATF-GAFI, FINANCIAL ACTION TASK FORCE ON MONEY LAUNDERING, REPORT ON MONEY LAUNDERING TYPOLOGIES 2003-2004, 19–23, *available at* http://www.fatf-gafi.org/dataoecd/19/11/33624379.pdf (discussing Politically Exposes Persons ("PEPs")); FATF-GAFI, FINANCIAL ACTION TASK FORCE, REPORT ON MONEY LAUNDERING TECHNOLOGIES 2001-2002, 12–14, *available at* http://www.fatf-gafi.org/dataoecd/29/35/34038006.pdf (discussing corruption and private banking).

110. These examples include 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. *See generally* U.S. MUTUAL EVALUATION REPORT, *supra* note 34.

111. FFIEC MANUAL, *supra* note 45, 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. *See, e.g.*, *id.* at Appendix G.

112. *Id.* at F-1.

available, such as known havens for money laundering or the names of senior foreign political figures subject to the heightened due diligence rules.[113]

Another serious problem is a lack of feedback on suspicious transaction reports actually filed by financial institutions and casinos to FinCEN.[114] According to a series of coinfidential interviews the author conducted with compliance officers at three U.S. banks, each believed it would be very helpful indeed to know if and why particular suspicious transaction reports resulted in a successful investigation. This would permit the bank to improve their monitoring and reporting systems by allowing them to review their systems based on actual successes and failures. However, FinCEN does not provide such feedback at all.[115]

FinCEN's methods are by no means unusual. A recent survey of Australia, the U.S., the United Kingdom, France, and certain other O.E.C.D. countries suggests that there is little useful information provided by domestic financial intelligence units to financial institutions and DNFBP, especially with respect to new money laundering techniques and trends within existing techniques.[116]

Without clear instructions in the Recommendations or Methodology on how to design and implement a preventive measures system, and without adequate guidance and feedback to supplement those standards, financial institutions and DNFBP still face a compliance supervisory process along with the threat of sanctions for non-compliance. Because the details of individual examinations are confidential, it is difficult to ascertain with any certainty how the supervisory process determines compliance. For example, FinCEN's published compliance actions[117] reveal very little detail as to nature of the preventive measures systems reviewed.[118] Nevertheless,

113. Sorcher, *Lost in Implementation*, *supra* note 3, at 415.

114. U.S. MUTUAL EVALUATION REPORT, *supra* note 34, at 65-68. 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, *U.S. and International Anti-Money Laundering Developments*, 43 INT'L LAW. 795, 802 (2009) [hereinafter Healy, *U.S. and International Anti-Money Laundering Developments*].

115. U.S. MUTUAL EVALUATION REPORT, *supra* note 34, at 65-68.

116. *See* Matthew H. Fleming, *UK Law Enforcement Agency Use and Management of SARs: Toward Determining the Value of the Regime*, 59 (2005), *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].

117. FinCEN, Compliance Actions, http://www.fincen.gov/news_room/ea/ (last visited Apr. 6, 2011).

118. "[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, *Bureaucracy to War*, *supra* note 70, at 1415.

a review of these actions clearly shows that breaches identified constitute clear failures in implementing the most basic of system requirements.[119] Also, in the course of conducting assessments of compliance with the FATF Recommendations, this author has reviewed hundreds of examination reports of financial institutions by supervisory authorities in six different countries, both developed and developing. As with the published FinCEN compliance actions, with no exception, the reports reveal an attention only to fundamental system requirements. In no instances had 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 DNFBP to perform relatively well with respect to recordkeeping and less well with respect to client identification, profiling, transaction monitoring, and suspicious transaction reporting. As will be demonstrated in Part II, this stands in sharp contrast to the duties of the private sector in enforcing the income tax laws. There, the rules are very clear, highly objective, and, not surprisingly, implemented far more effectively.

3. Economic and Regulatory Incentive Effects

There are a number of incentive effects that might militate both in favor of and against financial institutions and DNFBP seeking to implement an effective identification system. This section will begin by reviewing the conflicting incentives that arise when a policing function is privatized as an unfunded mandate.

Private sector persons may voluntarily assume policing responsibilities[120] when crimes directly affecting them are not being

119. *See, e.g.*, Doha Bank, New York Branch, Case Number 2009-1 (Dep't of Treasury April 20, 2009), *available at* http://www.fincen.gov/news_room/ea/files/Doha.pdf (wire transfer monitoring did not extend to multiple transfers, late filing of suspicious activity reports); NY Branch United Bank for Africa, Case Number 2008-3 (Dep't of Treasury April 28, 2008), *available at* http://www.fincen.gov/news_room/ea/files/UBAAssessment.pdf (no internal controls); El Noa Noa Corporation, Case Number 2008-2 (Dep't of Treasury April 14, 2008), *available at* http://www.fincen.gov/news_room/ea/files/ElNoaNoa.pdf (no implementation of written antimony laundering control program).

120. In the Anglo-Saxon world enforcement of the criminal law was almost entirely private up until the first half of the nineteenth 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, 921-24 (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. James F. Gilsinan, James Millar, Neil Seitz, James Fisher,

adequately addressed by the public sector. This is sometimes referred to as "self help."[121] As a general rule, the private, for-profit sector seeks to minimize costs as a way of maximizing profits. For this reason, one would expect that when a private sector actor chooses to assume the costs of law enforcement it would do so only when the benefits to the actor exceed the costs.[122] This calculus can be altered if the costs of such participation are paid wholly or in part by the public sector.[123] This can be accomplished through a general subsidy for carrying out a particular police function or though a system of bounty-hunting or reward for successfully assisting in the investigation or prosecution of a wrongdoer.[124] However, in both cases the calculus would be the same. The private sector person will carry out such a police function to the extent that total benefits from reducing the adverse effects of crime on the private sector person plus any subsidy or bounty exceed total costs involved.

The private sector can also be forced by law to take on the costs of private law enforcement with no compensation for doing so.[125] In most such cases, such unfunded mandates on the private sector are incentivized by applying penalties for failure to discharge adequately the required duties.[126] At least at first look, this appears to be the case with all of the preventive measures applicable to financial institutions and DNFBP.

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.

121. One of the most obvious historical examples is the private Pinkerton police force. Elizabeth E. Joh, *The Forgotten Threat: Private Policing and the State,* 13 IND. J. GLOBAL LEG. STUD. 357, 364-66 (2006) [hereinafter Joh, *The Forgotten Threat*]. Even such private policing can bring a public benefit. Clifford D. Shearing, *The Relation Between Public and Private Policing*, in MODERN POLICING, 339, 404 (Michael Tonry & Norval Morris eds., 1992), *cited in* Debra Livingston, *Police Discretion and the Quality of Life in Public Places: Courts, Communities, and the New Policing*, 97 COLUM. L. REV. 551, n.387 (1997).

122. This presumably would include costs of lobbying, bribing, etc. the public to protect the interests of the private actors.

123. Gilsinan et al. have referred to this as "the enthusiastic intelligence operative." Gilsinan, *The Role of Private Sector Organizations*, *supra* note 120, at 114-15.

124. James Fisher, Ellen Harshman, William Gillespie, Henry Ordower, Leland Ware, & Frederick Yeager, *Privatizing Regulation: Whistle-blowing and Bounty-Hunting in the Financial Services Industries*, 19 DICK. J. INT'L L. 117, 142-43 (2000) [hereinafter Fisher*, Privatizing Regulation*].

125. 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).

126. 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

If the private sector party were to see no direct benefit for 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 would seek to minimize costs as much as possible.[127] Those costs would include those involved in implementing the unfunded duties plus any sanctions for non-performance.[128]

To achieve 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. Certainly the more clear and objective the privatized enforcement requirement, the harder it would be for the private party to interpret "down" its duties.[129] However, any ambiguity would suggest that at least some of the interaction between private and public sectors involves the former attempting to restrict duties and the latter seeking to expand them. This general incentive structure suggests that financial institution and DNFBP would tend to minimize efforts to create effective systems.

There may be incentives working in the opposite direction, however. It may be that although they are required to implement preventive systems as an unfunded mandate, financial institutions and DNFBP may have some self-interest in implementing those mandates.

As a general matter, criminal law enforcement involves at least some degree of public goods.[130] The benefits accrue not only to one or more

---

costs on the party mandate to enforce them even if no money is appropriated to pay for those costs. John D. Graham, Paul R. Noe & Elizabeth L. Branch, *Managing the Regulatory State*, 33 FORDHAM URB. L.J. 953, 985 (2006). In the United States, The Unfunded Mandates Reform Act of 1995, 2 U.S.C. 1532 (Supp. 1995) requires both a qualitative and quantitative assessment of the anticipated costs and benefits of unfunded federal government mandates on state and local governments and on the private sector. Enacting unfunded mandates is also known as "cost-shifting." Thomas F. Burke, *The Rights Revolution Continues: Why New Rights are Born (and Old Rights Rarely Die)*, 33 CONN. L. REV. 1259, 1264 (2001).

127. With respect to the mandated privatization of financial regulation, Gilsinan et al. have referred to the private purveyors of police services as "the grudging informant." Gilsinan, *The Role of Private Sector Organizations*, *supra* note 120, at 113-14.

128. There may be some analogous incentive problems in the public sector, in that government agencies may tend not to focus their attention on issues or tasks that they believe are not central to their main mission. *See generally* JAMES Q. WILSON, BUREAUCRACY: WHAT GOVERNMENT AGENCIES DO AND WHY THEY DO IT (1989).

129. 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 Organizations*, *supra* note 120, at 114.

130. 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, *The Pure Theory of Public Expenditure*, 36 REV. OF ECON. & STATISTICS

persons who might suffer from any specific criminal act but to all persons, primarily through deterrence. For this reason, the benefits of self-help are shared by free riders, once again militating against the private sector spending any money on a mandate beyond the minimum to avoid sanctions.[131] However, in many instances there may be an overlap between public and private benefits.[132] While one would expect the private sector to try and control free-riders by focusing benefits 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.[133]

Financial institutions and DNFBP may voluntarily incur the costs of preventive measures for four 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.[134] It is better to spread the risk of default among a group of unconnected borrowers than to concentrate the risk in one; it is better to spread the risk of withdrawal of debt capital among a group of depositors than to concentrate it in one. Concentration risk also exists in both insurance and securities sectors for analogous reasons.[135] A key benefit of the client identification requirement could be to help financial institutions and DNFBP reduce this risk. The extent to which a

387, 387 (1954). "Which all enjoy in common" means that no one can (effectively) be excluded from the benefit. Thomas S. Ulen, *Rational Choice and the Economic Analysis of Law*, 19 LAW & SOC. INQUIRY 487, 492-93 (1994). The economist Dennis Mueller describes law enforcement as a "pure" public good. DENNIS MUELLER, PUBLIC CHOICE III, 10-11 (2003). However, some commentators have noted that selective enforcement, notably when racially based, is not a public good with respect to those who are victims of that enforcement. Paul Butler, *Starr Is to Clinton As Regular Prosecutors Are to Blacks*, 40 B.C. L. REV 705, 711 (1999).

131. In a group that provides itself with a public good, a "free rider" is one who contributes little or nothinng 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, *The Free Rider Problem: Experimental Evidence*, 43 PUBLIC CHOICE 3, 3 (1984).

132. Joh, *The Forgotten Threat*, *supra* note 121, at 375-83.

133. Ric Simmons, *Private Criminal Justice*, *supra* note 120, at 925.

134. BASEL COMMITTEE ON BANKING SUPERVISION, CUSTOMER DUE DILIGENCE FOR BANKS (2001), at paragraphs 14-15, *available at* http://www.bis.org/publ/bcbs85.pdf [hereinafter BASEL COMM., CUSTOMER DUE DILIGENCE].

135. International Association of Insurance Supervisors, Glossary, http://www.iaisweb.org/index.cfm?pageID=47&vSearchLetter=c## (defining "concentration risk"). It is far riskier to have a single insured than to spread the risk among many insured. FINANCIAL SERVICES COMMISSION, GUIDANCE NOTES CONCENTRATION RISK 13 (2008), *available at* http://www.fsc.gi/download/adobe/banking/noteconcrisk.pdf.

party would spend money to identify clients, including beneficial owners and controllers of those clients, would be based on a balance of costs to benefits of avoiding such concentration risk. While neither is immediately obvious, at least some incentive would exist for at least certain types of financial institutions to implement this requirement.

The next form of risk is reputational risk. Reputational risk is risk caused by events adversely affecting the reputation of an enterprise, particularly a financial institution.[136] Banking regulators have long hypothesized that known or assumed use of banks by criminals could result in adverse consequences as customers and investors react by shunning the institution. Reputational risk also faces other persons, financial and nonfinancial.[137] Although discussing sanctions against Iran rather than money laundering and terrorism financing *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." [138] Treasury Deputy Assistant Secretary Daniel Glaser further noted 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."[139] Therefore, implementation of anti-money laundering and terrorism financing standards by banks could have direct financial benefits by avoiding such reputational risks.

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 on the use of banks by money launderers show no change in stock price from those stories.[140] While additional research is needed, there is doubt that financial institutions and DNFBP would weigh heavily concerns over reputational risk.

---

136. "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." BASEL COMM., CUSTOMER DUE DILIGENCE, *supra* note 134, at para. 11. 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. SCHOTT, REFERENCE GUIDE, *supra* note 9, at II-5.

137. THE ECONOMIST INTELLIGENCE UNIT, REPUTATION: RISK OF RISKS 2 (2005) (arguing that maintaining a good reputation is the most important and difficult task facing senior risk managers).

138. Quoted in Orde F. Kittrie, *New Sanctions for a New Century: Treasury's Innovative Use of Financial Sanctions*, 30 U. PA. J. INT'L L. 789, 816-17 (2009).

139. *Id.*

140. Michael Levi, Lecture to International Monetary Fund, Washington, D.C. (2003).

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 may not be effective *even if properly implemented*.[141] If they were not, there would be little reputational risk benefit to spending money to implement them. And, as discussed earlier, 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.[142]

While there is speculation as to the effects of reputational risk in incentivizing financial institutions to implement their preventive measures responsibilities, there may also be significant disincentives. Financial institutions may see a benefit in being known to be lax in implementing anti-money laundering duties in that they may attract criminal clients who wish to avoid being caught.[143] Much of the current struggle by developed countries to eliminate bank secrecy in offshore financial centers has focused on this perceived benefit to financial institutions that offer locations to hide criminal proceeds, such as in tax evasion.[144] It is by no means certain which incentive, the downside risk of a bad reputation or the upside risk of a bad reputation, is stronger.

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.[145] 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. Unfortunately little publicly available information exists on how financial institutions and DNFBP seek to prevent financial fraud, an issue that is not addressed in anti-money laundering evaluations. A major reason for the absence of such information is concern by private parties over protecting propriety systems and concern over competition.[146] However, insight into anti-fraud client identification

141. This issue is discussed *infra in* Part III.

142. *See supra* note 88 and accompanying text.

143. This argument applies only to money laundering and not terrorism financing, where adverse reputation is likely to be far greater than any possible financial benefits from having terrorists as clients. But that's just a guess.

144. *See* Gordon, *On the Use and Abuse of Standards for Law*, *supra* note 15, at 515–18, 563–64; *see also* Linnley Browning, *Swiss Banker Blows Whistle on Tax Evasion*, N.Y. TIMES, January 18, 2010, at B1 (describing political fallout over the use by U.S. citizens of Swiss banks to engage in tax evasion).

145. BASEL COMM., CUSTOMER DUE DILIGENCE, *supra* note 134, at para. 12.

146. This absence of information is similar to problems in identifying information on how the private sector implements preventive measures. *See infra* notes 195-202 and accompanying text.

and account monitoring can be gained from examining systems provided by third party services to financial institutions. 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."[147] 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 separate and different.[148]

That being noted, fraud committed against a financial institution and money laundering and terrorism financing implemented by a financial institution are quite different. In the first instance the financial institution is the victim; in the second, the financial institution is the medium through which the crime is perpetrated.[149] The vast majority of criminal proceeds do not involve fraud against banks.[150] While there are many possible origins of terrorism financing, bank fraud is only one of them and is unlikely to be a significant source.[151] For that reason, one would expect financial institutions and DNFBP to focus not on money laundering or terrorism financing risks, but on those that directly adversely affect them, like fraud.[152] A key aspect of any anti-fraud program found in a preventive measure is the identification and profiling of potential clients and employees. Among the most common form of customer fraud against

147. This includes 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. *See generally* Guardian Officer, GLOBALVISION SYSTEMS, 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 (Feb. 20, 2010).

148. *Id.*

149. IMF, FINANCIAL SYSTEM ABUSE, FINANCIAL CRIME AND MONEY LAUNDERING—BACKGROUND PAPER 40 (2001), *available at* http://www.imf.org/external/np/ml/2001/eng/021201.pdf [hereinafter IMF, MONEY LAUNDERING BACKGROUND PAPER].

150. PETER REUTER & EDWIN M. TRUMAN, CHASING DIRTY MONEY: THE FIGHT AGAINST MONEY LAUNDERING 22 (2004) [hereinafter REUTER & TRUMAN, THE FIGHT].

151. *See* COUNTERING THE FINANCING OF TERRORISM 91-206 (Thomas J. Biersteker & Sue E. Eckert eds., 2008).

152. "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*." 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. CRIM. 3, 6 (2008).

banks are creditor fraud and wire and check fraud.[153] Simple background checks could identify persons known to have engaged in such activity. In addition to identifying known fraudsters, financial institutions may be able to monitor types of customers and transactions to uncover known fraudulent patterns. For example, one recent creditor fraud involved people posing as wealthy dentists who took out loans to purchase speed boats. The fraudsters forged various documents including titles to non-existent boats, which they used for security to obtain the loans. Once this scheme was uncovered in one of the bank's branches the bank was able to uncover similar schemes in other branches.[154] The bank had every incentive to uncover such frauds against the bank. These incentives do not, however, extend to possible money laundering or terrorism financing.

Fraud detection can be assisted by sharing doubts about client bona fides with financial intelligence units. Their access to extensive databases including police records, immigration and customs records, tax records, and supervisory findings[155] make them particularly effective at uncovering fraud patterns among large numbers of financial transactions among different financial institutions. As a result, some units, including FinCEN, are tasked not only with anti-money laundering and terrorism financing duties but also with preventing fraud against financial institutions. The difference between reporting possible fraud and possible money laundering or terrorism financing is demonstrated by examining the types of reports filed to financial intelligence units. For example, in the United States, a significant percentage of suspicious transaction reports filed with FinCEN are not concerned with money laundering or terrorism financing but with possible fraud, and are identified as such on the report.[156]

While additional research needs to be undertaken there does appear to be some significant anti-fraud benefit to financial institutions and DNFBP in client identification and client profiling. There may also be some benefit to monitoring transactions to see if they fit any known patterns indicating fraud, and to report those to financial intelligence units. However, this

153. IMF, MONEY LAUNDERING BACKGROUND PAPER, *supra* note 149, at 40. 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. *See* FinCEN, Bank Secrecy Act Records Lead to Funds for Restitution in Insurance Fraud, *available at* http://www.fincen.gov/law_enforcement/ss/html/014.html; s*ee also* FATF, Money Laundering and Terrorist Financing in the Securities Sector 48– 53 (2009), *available at* http://www.fatf-gafi.org/dataoecd/32/31/43948586.pdf.

154. Confidential interview with bank compliance officer in Cleveland, OH (Apr. 12, 2009).

155. IMF, FINANCIAL INTELLIGENCE UNITS, *supra* note 71, at 58.

156. 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 19, at 4.

would not usually extend to client identification or transaction monitoring to detect money laundering or terrorism financing.

The last possible risk to be avoided, legal or regulatory risk, arises from the possibility that financial institutions and DNFBP may suffer enforcement actions such as fines and criminal liabilities for breaching anti-money laundering or terrorism financing laws or regulations.[157] However, these are risks for failure to implement burdens imposed by the state for law enforcement purposes, not imposed to benefit the financial institution.[158] There would be direct benefits to financial institutions and DNFBP if they paid fewer fines, but this would have to be balanced against the costs of implementing preventive measures, including indirect costs.

However, the application of sanctions against *customers* creates a strong *disincentive* to report possible laundering. As noted, a principal public benefit of anti-money laundering rules is that they allow the confiscation of criminal proceeds.[159] If such proceeds are on deposit or otherwise loaned to or invested in a financial institution or DNFBP, the confiscation of those proceeds would actually injure that enterprise by depriving it of capital. This could be a significant indirect cost. The larger the magnitude of the proceeds, the greater would be the injury to the enterprise. Given this potentially significant incentive, a purely profit-maximizing financial institution or DNFBP would seek to follow their preventive measures obligations only as far as to avoid sanctions for non-compliance, but would stop short of the point where they detected and reported actual money laundering, at least with respect to criminal proceeds that form part of the enterprise's capital base.

On balance, there is strong suggestion that financial institutions and DNFBP will see risk-reduction benefits from implementing customer identification and profiling rules and some from fraud-related transaction monitoring and reporting. However, there appears to be no obvious net self-benefit for anti-money laundering transaction monitoring or 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.

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.

157. BASEL COMM., CUSTOMER DUE DILIGENCE, *supra* note 134, at para. 13.

158. Richard Gordon, *Anti-money-laundering Policies: Selected Legal, Political, and Economic Issues*, 1 CURRENT DEV. IN MONETARY & FIN. L. 405, 407 (1999).

159. *See supra* note 5 and accompanying text.

Exactly how much is difficult to quantify.[160] At least with respect to banks, transaction monitoring appears to be the greatest area of expenditure.[161] Given that transaction monitoring appears to provide little direct benefit to the financial institution itself (that is, compared to customer identification and profiling, which may help prevent fraud), this does not bode well for implementation.

In 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 one commentator has referred to as a "cottage industry of consultants."[162] Such outsourcing can have advantages, such as reducing costs through economies of scale and improving quality through competition.[163] However, smaller institutions may be buying scaled-down "anti-money laundering lite" software,[164] which may not be a good sign with respect to effective implementation. At any rate, implementation costs certainly must have a negative effect on implementation when placed into the cost/benefit considerations of financial institutions and DNFBP.

That being said, unfunded mandates do have the benefit of shifting costs from the public to the private sector. This can have some benefits, as well as some potential downsides that will be discussed at greater length below.[165]

As noted earlier, there are significant potential regulatory incentives to compliance.[166] However, these incentives, based on fines and other forms of compliance action, have been applied to failures to implement basic requirements (such as no customer identification system, no profiling system, no transaction monitoring).[167] None appears to have been based on a results-focused failure of the system. It is therefore not obvious how these

160. Various attempts have been made, however. According to some estimates 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 70, at 1413. Presumably these costs have increased. *See also* Sorcher, *Lost In Implementation*, supra note 3, at 396 (noting that banks have significantly increased their spending on AML/CFT procedures).

161. KPMG, ANTI–MONEY LAUNDERING SURVEY, *supra* note 103, at 8.

162. Zaring & Baylis, *Bureaucracy to War*, *supra* note 70, at 1413.

163. 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 BENSON, TO SERVE AND PROTECT, *supra* note 120, at 27. This suggests greater risk taking and perhaps innovation as well as greater quality control and lower costs of through greater efficiencies. *Id*.

164. *See* Adams, *Diligence is Getting Pretty Pricey*, *supra* note 88.

165. *See infra* notes 189-194 and accompanying text.

166. *See supra* note 70 and accompanying text.

167. *Id.*

would incentivize financial institutions to implement *effective* preventive measures. As a result, with unclear and subjective written requirements, often unhelpful guidance and feedback, and a lack of clear incentives for effectiveness, one would expect that financial institutions and DNFBP would not to do a particularly good job in implementing preventive measures. As will be discussed in Part II, this is very different from how the private sector implements its tax administration duties, where requirements are not only clearly stated but where incentives for effectiveness are quite clear.

As noted earlier, neither compliance reports nor sanctions reported by supervisory authorities discuss in any detail the design of compliance systems.[168] Financial institutions and DNFBP also do not publicize exactly how they implement these requirements.[169] However, some commentators have provided a list of actions that private firms could take to implement their preventive measures duties in the most effective manner possible.[170] This "wish list" is not a description of what firms actually implement—only what they could implement assuming that cost was no object. Among these is link analysis.[171]

Link analysis is a technique used to find associations within data that might have relevance to the particular research question.[172] Link analysis explores associations within collections of data.[173] Increasing the number of

---

168. *Id.*

169. An important barrier to learning more about how firms actually implement their preventive measures requirements is a concern over protecting proprietary information in the context of competitive concerns. 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, *available at* http://www.pwc.com/lu/en/anti-money-laundering/case.jhtml (providing almost no detail on preventive measures system recommended by outside consultant).

170. G. S. Vidyashankar, Rajesh Natarajan, Subhrangshu Sanyal, Mine Your Way to Combat Money Laundering, Part 1, DM Review Special Report, October 2007, *available at* http://www.information-management.com/specialreports/20071002/1093412-1.html [hereinafter Vidyashankar *et al*., Mine Your Way Part 1]; G. S. Vidyashankar, Rajesh Natarajan, Subhrangshu Sanyal, Mine Your Way to Combat Money Laundering, Part 2, DM Review Special Report, October 2007, *available at* http://www.information-management.com/specialreports/20071009/1093416-1.html [hereinafter Vidyashankar *et al*., Mine Your Way Part 2].

171. Vidyashankar *et al.*, Mine Your Way Part 1, *supra* note 170; Vidyashankar *et al*., Mine Your Way Part 2, *supra* note 170.

172. Cuellar, *Criminal Law*, *supra* note 3, at 368.

173. FINCEN, FEASIBILITY OF A CROSS-BORDER ELECTRONIC FUNDS TRANSFER REPORTING SYSTEM UNDER THE BANK SECRECY ACT 10 (October 2006), *available at* http://www.fincen.gov/news_room/rp/files/CBFTFS_Complete.pdf [hereinafter FINCEN, CROSS-BORDER ELECTRONIC FUNDS]; *see also* Cuellar, *supra* note 3, at 368. Much of the information in the following two paragraphs has been provided by Boudewijn Verhelst. Verhelst e-mail, *supra* note 20.

data sets available increases the number and types of links that can be identified.

There are a number of different types of data set 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 that which is found in business directories like Dunn and Bradstreet. Links to data that include money laundering or terrorism financing indictors, 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 that they constitute criminal proceeds or laundering. This suspicion could be raised further if person A owns or controls company B and company B itself has no known business. 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 DNFBP are restricted in their access to some useful data sets, an issue that will be discussed below. As will be seen in Part II, link analysis is used with great effectiveness by the public sector in tax administration.

Such use of descriptive links and analysis is also described as data mining and the use of algorithms.[174] Such algorithms can be based on typical laundering typologies or "red flag" indicators provided by supervisory authorities and the Financial Action Task Force. However, as will be discussed below, such algorithms appear to be based on idiosyncratic judgment rather than empirically sustainable classifications.[175]

Empirically derived algorithms are based on regression analysis or discriminant function analysis. Regression analysis is a technique for

174. Vidyashankar *et al.*, Mine Your Way Part 2, *supra* note 170.

175. FREDERICK SCHAUER, PROFILES, PROBABILITIES, AND STEREOTYPES 92–101 (2003).

discovering the relationship between a dependent variable 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 the dependent variable can also be reflected in a probability distribution. Typically, one begins with a hypothesis that the presence and magnitude or a particular factor (the independent variable) is a predictor of something (the dependent variable). One then tests the hypothesis using factual data and statistical analysis.[176] 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 of determining 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.[177] 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 made on human hunches or "idiosyncratic assessments" that have no proven statistical accuracy.[178] As will be seen in Part II, link discriminant function analysis is used with great effectiveness by at least some tax administrations.

Given that typologies and red flags that supervisory authorities and others provide do not appear to be scientifically derived, it seems unlikely that private firms, which are primarily concerned about controlling regulatory/legal risk, would themselves use regression analysis. In addition,

176. *See generally* Alan O. Sykes, *An Introduction to Regression Analysis*, *in* CHICAGO LECTURES IN LAW & ECONOMICS (Eric Posner ed., 2000), *available at* http://www.law.uchicago.edu/files/files/20.Sykes_.Regression.pdf (describing linear and non-linear regression analysis).

177. *See generally* John Poulsen & Aaron French, *Discriminant Function Analysis* (2003), *available at* http://userwww.sfsu.edu/~efc/classes/biol710/discrim/discrim.pdf (describing discriminant function analysis).

178. SCHAUER, *supra* note 175, at 92.

private sector entities lack access to important data sets, such as confidential data from other financial institutions and DNFBP and private or classified government data (discussed below in Section 4). Also, managing large sets of data is simply difficult to do.[179]

As noted above at least some financial institutions contract out some of their customer identification and client monitoring programs to third party service providers.[180] 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.[181] Firms can also supply transaction monitoring services. One firm "monitors and detects" suspicious transactions "across all business lines" using "a fully integrated dynamic and adaptive multidimensional intelligent engine [which] detects suspicious activities" using "risk modeling" and "risk-based algorithms" to "analyze and investigate suspicious activities effectively and efficiently."[182] But as contractors to those primarily responsible for implementing preventive measures, there is little reason to believe that such third party provider 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 financial institutions and perhaps DNFBP use such services, and some contract for "lite" versions.[183] Exactly why some financial institutions and DNFBP use contractors 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 is likely that supervisors will not sanction firms for non-compliance.[184]

Private sector entities appear to file far too many suspicious transaction reports, providing a huge flow of false positives. If a financial institution is usually sanctioned 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

179. Vidyashankar et al., *Mine Your Way Part 2*, *supra* note 170 ("Analysis of such huge volumes imposes a huge computational burden….").

180. *See supra* notes 162-164 and accompanying text.

181. *See, e.g.*, World-Check Online, http://www.world-check.com/online/ (last visited Apr. 6, 2011).

182. American Bankers Association, PATRIOT OFFICER GlobalVision Systems, Inc., http://www.aba.com/CAB/cab_patriotofficer.htm (last visited Apr. 6, 2011).

183. *See supra* note 164 and accompanying text.

184. Confidential interviews with compliance officers at financial institutions, *supra* note 154.

institutions and DNFBP to apply too little scrutiny and to over-report.[185] Currently, in many key jurisdictions, there have been considerable increases in suspicious transaction reporting.[186] Because so few of these reports result in actual prosecutions, the result has often been a general flooding of financial intelligence units with essentially "defensive" suspicious transaction reports.[187] This can generate information overload and generally clog the criminal investigations system with too many false positives.[188]

There are a few possible other good and bad negative effects. Some scholars have argued that the private sector is more likely to act self-interestedly than the public sector, and if so, the private sector may be more likely to commit to a higher level of unethical acts.[189] One type of unethical act could be racial or other invalid profiling. While profiling based on purely statistical analysis of empirical data 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.[190] Given that all typologies reports, red flags, and other

185. *See generally* Elod Takats, *A Theory of 'Crying Wolf': The Economics of Money Laundering Enforcement* 4 (Int'l 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). Flooding financial intelligence units with too many reports could also help bury those that are actually useful, benefiting reverse reputational risk and protecting client assets from seizure.

186. This conclusion is supported by specific studies of the United States and the United Kingdom. *See* Cuellar, *supra* note 3, at 396 (describing increases in SARing in the United States); STEPHEN LANDER, SERIOUS ORGANISED CRIMES AGENCY, 13 (2006), *available at* http://www.soca.gov.uk/downloads/SOCAtheSARsReveiw_Fina;_Web.pdf; Michael Levi & Peter Reuter, *Money Laundering*, 34 CRIME & JUST. 289, 313 (2006).

187. Verhelst e-mail, *supra* note 20. ("There is no indication that FinCEN . . . knows how to manage all of these reports. In fact, the former director of FinCEN complained in 2004 that too many of these SARs were being filed by banks. The haphazard nature of the fines that FinCEN has imposed has led some observers to question1whether the agency has a policy in place to sort through each of the reports."); Zaring & Baylis, *supra* note 70, at 1415 (citations omitted). According to one source, a compliance officer in French financial institution noted that if "[y]ou want to stay out of trouble? Then file a report." Gilles Favarel-Garrigues, Thierry Godefroy, & Pierre Lascoumes, Sentinels in the Banking Industry, *Private Actors and the Fight against Money Laundering in France*, 48 BRIT. J. CRIMINOLOGY 1, 11 (2008) [hereinafter Favarel-Garrigues *et al*., *Private Actors*].

188. LANDER, *supra* note 186; Levi & Reuter, *supra* note 186, at 313; Fleming, UK Law Enforcement, *supra* note 116, at 10, 35-6; REUTER & TRUMAN, THE FIGHT, *supra* note 150, at 101-2.

189. This is not to suggest that public sector employees are always more ethical, only that they tend to be more so than the private sector. *See* Simmons, *Private Criminal Justice*, *supra* note 120, at 978–79.

190. SCHAUER, *supra* note 175, at 92–101. Even those who strongly oppose racial profiling for national security purposes do so 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, 138–40 (2010).

guidance is based on informed guesswork one can reasonably speculate that financial institutions and DNFBP are using unscientific profiling to target certain categories of client to avoid the application of sanctions. If the adversely affected clients provide relatively small profits to the financial institutions or DNFBP the likelihood that they would simply be dropped as a client increases dramatically. This may result in reduced access to the financial system by those clients.[191]

One area where there is some evidence that this is happening is with charities. Special Recommendation VIII suggests that some charities appeared to be involved in terrorism-financing transactions. This was emphasized repeatedly in material that could be referenced by financial institutions, their supervisors, and law enforcement, including FATF reports and guidance issues by national regulators.[192] There is no reason to believe that supervisors believe that all charities are somehow tainted. But if regulated financial institutions and DNFBP believe that having fewer charity clients will result in less of a chance that sanctions will be applied to them, financial institutions and DNFBP may be less likely to accept them as clients, particularly if they are low-profit clients. Although this would not be the intent of supervisors, this would reduce charities' access to the formal financial system. There is some evidence that this is in fact happening.[193] 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 increasing prices the institutions charge clients, reducing net profits, or (most probably) a mix of the two. Higher financial institution prices can have significant and adverse public policy effects, such as decreasing access to financial services by low income clients.[194]

---

191. 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 with bank compliance officer in Cleveland, *supra* note 154.

192. Gordon, *Trysts or Terrorists*, *supra* note 4, at 718–19.

193. *See generally* Nina J. Crimm, *High Alert: The Government's War on the Financing of Terrorism and Its Implications for Donors, Domestic Charitable Organizations, and Global Philanthropy*, 45 WM. & MARY L. REV. 1341 (2004) (discussing extensively the liabilities imposed by the U.S. on charitable donations by anti-terrorism financing laws).

194. JENNIFER ISERN & DAVID PORTEOUS, AML/CFT REGULATION: IMPLICATIONS FOR FINANCIAL SERVICE PROVIDERS THAT SERVE LOW INCOME PEOPLE 9–16 (2005) (discussing how increased costs due to implementation of AML/CFT regulations may reduce the supply of affordable financial services to low-income persons).

4. Objective Capacity

The issue addressed in this section is the private sector's capacity or access to information needed for it effectively to implement its preventive measures. Whether state authorities like financial intelligence units have such capacity and access is addressed in section E.

Financial institutions and DNFBP have access to a considerable amount of data required for effective implementation of preventive measures. As a point of access to the financial system, financial institutions and DNFBP can demand, inspect, and copy client identity documents.[195] They also have access to transactions of their own clients and can easily keep records of those transactions.[196] Because of relative ease of access to certain databases such as company registries, business registries (e.g. Dunn and Bradstreet), court records, and conceivably others, they may be able to detect false documentation and to make some link analysis.[197] Finally, financial institutions in particular are expert at how to store money, move it, and guard it.[198] 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.[199]

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 of the legal person or arrangement is relatively easy.[200] Even though Recommendations 33 and 34 require states to provide such information to the public, they are often incapable of doing so.[201] As a result, the identification of beneficial owners and controllers is often completed in an unsatisfactory fashion.[202]

---

195. This may be a principal reason that client identification is relatively successful. *See supra* note 81 and accompanying text.

196. This may be a principal reason that record-keeping is relatively successful. *See supra* note 80 and accompanying text.

197. Verhelst e-mail, *supra* note 20.

198. Mariano-Florentino Cuellar, *The Mismatch Between State Power and State Capacity in Transnational Law Enforcement*, 22 BERKELEY J. INT'L L. 15, 25 (2004).

199. *See* discussion of link analysis, data mining, and algorithm development *supra* notes 174-181 and accompanying text.

200. *See generally* FATF, THE MISUSE OF CORPORATE VEHICLES, INCLUDING TRUST AND COMPANY SERVICE PROVIDERS (2006) (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).

201. *See e.g.* U.S. MUTUAL EVALUATION REPORT, *supra* note 34, at 57; AUSTRIA MUTUAL EVALUATION REPORT, *supra* note 80, at 221–2, 225; AUSTRALIA MUTUAL EVALUATION REPORT, *supra* note 80, at 121-3; CANADA MUTUAL EVALUATION REPORT, *supra* note 80, at 250, 253; U.K. MUTUAL

Another key issue involves access to sufficient data to perform adequate link analysis. As noted earlier, successful link analysis depends on the ability to access as much data as possible. The first problem involves transaction data. Financial institutions and DNFBP are aware only of the transactions of their own clients and not of clients of other financial institutions or DNFBP. If a client engages in a transaction with a client of another enterprise the chain or link is severed. If financial institutions and DNFBP 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.[203] 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 person's 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. It would be difficult to justify the added costs of such a bizarrely redundant system.

The second problem involves access to other data, such as confidential government 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 tax records, police records, immigration and customs records, vehicle registries, and supervisory findings.[204]Also absent would be previously filed suspicious transaction reports. Under the Recommendations, such reports are treated as strictly confidential, not only to protect client's legitimate privacy interests, but to ensure that there is no tipping off.[205]

Next, typologies and red flag indicators may help in designing algorithms, but if those algorithms are not based on appropriate statistical analysis they will be of 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 at least greatly limited, access to

---

EVALUATION REPORT, *supra* note 80, at 236, 239; HONG KONG CHINA MUTUAL EVALUATION REPORT; *supra* note 80, at 164-5, 167.

202. 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* World Bank, *Component 1 Analytical Spreadsheet* (February 1, 2010), on file with the author of this Article.

203. Sharing client information with both domestic and foreign law enforcement authorities is another matter. FATF 40 Recommendations, *supra* note 3, at Recommendation 40; Methodology, *supra* note 10, at Criterion 40.4.1.

204. Verhelst e-mail, *supra* note 20.

205. FATF 40 Recommendations, *supra* note 3, at Recommendation 14.

the dependent variable: a higher probability of money laundering or terrorism financing. In fact, a principal complaint of financial institutions and DNFBP is that they receive no feedback as to whether their suspicious transaction 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.[206] Without this most basic form of feedback, it is impossible to determine if a 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 financial institutions and at least some DNFBP have expertise in financial transactions, there is no reason to believe that they are experts in criminal investigations.[207] This raises considerable doubt that they would be able to form the necessary hypotheses between dependent and independent variables, let alone test them.

5. Other Issues

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 budget. This frequently has political benefits, even if the result is expressed in higher private sector prices. There may be other cost-savings involved in private unfunded mandates.[208] We do not know if these were a motivation behind the setting up of the current system. Another reason may be that the private sector has better, or at least more easily obtainable, access to certain key information than does the public sector.[209]

There is one other key issue. The fact that the public sector does not use empirically-based algorithms means there are no specified independent

206. EUROPEAN COMMISSION, DIRECTORATE-GENERAL, JUSTICE, FREEDOM AND SECURITY: FINAL REPORT ON FEEDBACK 30, 53 (2007). *See, e.g.*, AUSTRIA MUTUAL EVALUATION REPORT, *supra* note 80, at 144 (no up-to-date guidance); AUSTRALIA MUTUAL EVALUATION REPORT, *supra* note 80, at 90 (inadequate feedback on suspicious transaction reports filed); CANADA MUTUAL EVALUATION REPORT, *supra* note 80, at 262 (no feedback on suspicious transaction reports filed) U.K. MUTUAL EVALUATION REPORT, *supra* note 80, at 148 (no direct feedback); *but see* HONG KONG CHINA MUTUAL EVALUATION REPORT, *supra* note 80, 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 104, at 8.

207. Gordon, *Trysts or Terrorists*, *supra* note 4, at 737.

208. 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).

209. This is not unique to preventive measures implementation. *See, e.g.*, Fisher, *Privatizing Regulation*, *supra* note 124, at 141; William E. Kovacic, *Whistleblower Bounty Lawsuits as Monitoring Devices in Government Contracting*, 29 LOY. L.A. L. REV. 1799, 1821 (1996).

variables that trigger investigations. If there were, and these were known by money launderers and terrorists, they could change their tactics and patterns (i.e. their independent variables) to reduce the likelihood that they would be investigated and, therefore, caught.

E. Public Sector Successes and Failures

The principal 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.[210] Through examination and analysis, the financial intelligence unit attempts to distinguish truly suspect transactions from those that are only "benignly" unusual.[211] In effect, the financial intelligence unit must determine which "suspicious" reports are *really* suspicious.

Dividing the task of determining suspicious and *really* suspicious transactions between the private sector and public financial intelligence units usually begins with the receipt of a suspicious transaction report, after which the financial intelligence unit engages in a two-part analysis. In the first part, known as 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.[212] 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 databases to which the private sector has access.[213] It can also have access to databases to which the public has no access, such as tax records, police records, immigration and customs records, vehicle registries, and supervisory findings.[214]

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*.[215] The same is true with respect to similar information from private sector persons in foreign

210. SCHOTT, REFERENCE GUIDE, *supra* note 9, at VII.

211. *Id.*

212. *Id.* at VII-6 to 7; IMF, FINANCIAL INTELLIGENCE UNITS, *supra* note 71, at 57–58.

213. *See supra* note 195 and accompanying text.

214. Verhelst e-mail, *supra* note 20.

215. FATF 40 Recommendations, *supra* note 3, at Recommendation 10.

jurisdictions.[216] 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, the United States, Canada, and Australia, as well as some developing countries like the Philippines, require automatic reporting of certain types of financial transactions to financial intelligence units.[217] One type of transaction that results in automatic reporting is cash transactions, which require financial institutions or DNFBP to report all cash transactions greater than a certain amount. There are good reasons for having such a rule. In the paradigm case of laundering the proceeds of illegal drug sales, traffickers tend to be paid in cash.[218] In order to avoid use of large amounts of cash (which can be bulky and can invite unwanted attention) the criminal needs to enter the cash into the formal financial system via a financial institution. Doing so is referred to as the "placement stage."[219] One of the first anti-money laundering 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.[220] The United States, for example, has long had automatic cash transaction reporting rules (for amounts in excess of $ 10,000), as have a number of other countries.[221] Another type of automatic reporting 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)[222] or all transactions regardless of amount

216. FATF 40 Recommendations, *supra* note 3, at Recommendation 40; Methodology, *supra* note 10, at Criterion 40.4.1.

217. U.S. MUTUAL EVALUATION REPORT, *supra* note 34, at 148; CANADA MUTUAL EVALUATION REPORT, *supra* note 80, at 159; AUSTRALIA MUTUAL EVALUATION REPORT, *supra* note 80, at 86–87; REPUBLIC OF THE PHILIPPINES: DETAILED ASSESSMENT REPORT ON ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM 145 (2009) (copy on file with the author).

218. See *supra* note 4.

219. SCHOTT, REFERENCE GUIDE, *supra* note 9, at I-7.

220. Gordon, *Trysts or Terrorists*, *supra* note 4, at 708.

221. U.S. MUTUAL EVALUATION REPORT, *supra* note 34, at 148.

222. 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. CANADA MUTUAL EVALUATION REPORT, *supra* note 80, at 159. *See also* FINTRAC, *What Must be Reported? Electronic Funds Transfer*, *available at*
http://www.fintrac-canafe.gc.ca/reporting-declaration/Info/rptEFT-eng.asp.

(Australia).[223] An analysis by FinCEN suggested that such data, by extending link analysis, can have significant benefits in uncovering laundering.[224] FinCEN recently proposed a regulation requiring such reporting in the United States.[225] FinCEN sought to address concerns of reporting persons that such reporting would significantly raise costs in part by calling for "increasing the use of technology to automate and standardize the transfer of data from financial institutions, FinCEN, and law enforcement agencies." [226]

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 [financial intelligence unit] 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.[227]

Based on such analysis, the financial intelligence unit may or may not disseminate a report for further investigation.[228]

Another important function of the financial intelligence unit is strategic analysis, or developing relevant knowledge on techniques of laundering or terrorism financing. Examples include "the identification of evolving criminal patterns in a particular group or the provision of broad insights into emerging patterns of criminality."[229] 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,

---

223. AUSTRALIA MUTUAL EVALUATION REPORT, *supra* note 80, at 86; *see also* AUSTRAC, *International funds transfer instructions*, *available at* http://www.austrac.gov.au/inter_funds_transfer.html.

224. FinCEN, CROSS-BORDER ELECTRONIC FUNDS, *supra* note 72, at 5-10.

225. Cross-Border Electronic Transmittals of Funds, 75 Fed. Reg. 60,377 (proposed Sept. 30, 2010).

226. *Id.* at 60,378.

227. IMF, FINANCIAL INTELLIGENCE UNITS, *supra* note 71, at 59.

228. *Id.* at 60.

229. SCHOTT, REFERENCE GUIDE, *supra* note 9, at VII-7; IMF, FINANCIAL INTELLIGENCE UNITS, *supra* note 71, at 59-60.

typologies etc. for use by financial institutions and DNFBP.[230] This generally follows the system used by FinCEN in the United States. [231]

However, as is the case with the private sector, financial intelligence units do not use regression analysis or discriminant function analysis to test hypotheses.[232] 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. Although financial intelligence units can request and receive records on *specific* transactions, they do not automatically have access to all transactions. Because financial intelligence units do not use these analytical tools, methodologies and "red flags" are made on human hunches or "idiosyncratic assessments" that have no proven statistical accuracy.[233] As noted earlier, Part II will discuss how some tax administrations use statistical analysis to select income taxpayers and returns for audit.

Another failure of financial intelligence units is 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. Typologies and red flags are not based on scientific analysis.[234] Exactly why they do not is open to some speculation. Perhaps the most likely reason for not assisting in the design of preventive measures systems is that they do not know the best designs. They are not, after all, in the business of designing such systems but only of analyzing suspicious transaction reports. Most importantly, they do not have access to all financial transaction data, which is needed to design such systems effectively. It may also be that if they provide too much information on how to find potential launderers and terrorists to the private sector, that information might get back to the actual launderers and terrorists. In other words, the system as it now stands is inherently contradictory: the private sector needs the financial intelligence unit's knowledge to design and implement effective preventive measures systems, but the financial intelligence unit dare not provide too much information for fear of such information actually helping criminals and terrorists.

F. Summary and Conclusions

Preventive measures for money laundering and terrorism financing have not worked well. This is because the current system is based on a

230. IMF, FINANCIAL INTELLIGENCE UNITS, *supra* note 71, at 60.

231. U.S. MUTUAL EVALUATION REPORT, *supra* note 34, at 126-35.

232. Verhelst e-mail, *supra* note 20.

233. SCHAUER, *supra* note 175, at 92.

234. *See supra* text accompanying note 182.

faulty theory of how such duties should be divided. The preventive measures standard—by requiring financial institutions and DNFBP to design and implement requirements that are poorly described, expensive, and unfunded—invites failure. Given that the private sector's main motive is profit, theory would predict that it would seek to reduce its costs by spending as little as possible on implementing those requirements. Because of their subjective nature, it is possible for the private sector to define downward its duties without fear of sanction. In addition, the requirements describe a mandate that the private sector has little objective capacity to implement, even if it wanted to.

The Recommendations are, with respect to designing and implementing a profiling, monitoring, and suspicious transaction reporting system, too vague and subjective. Also, there is little feedback or assistance from the public sector in refining these responsibilities. While it is no doubt possible to make the wording clearer, as well as to implement improved guidance and feedback it is difficult to see how to make the system itself *significantly* less subjective and open to interpretation. Governments, by having put the burden of designing these systems on to the private sector, have never had to perform the necessary research and analysis to come up with effective systems themselves, suggesting they probably do not now have adequate expertise and essential data to do so. And even if they did, they cannot provide too much information for fear of such information actually helping criminals and terrorists. This inherent contradiction in the system makes a resolution more or less impossible.

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 less comprehensive or 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. However, these could be expensive and could act as a deterrent to filing suspicious transaction reports.

One 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 would be no need for the private sector to design or implement a selection system. The current system requires the government to examine reports from the private sector and determine which of those reports should be further investigated; in effect, to determine which "suspicious" reports are *really* suspicious. Dividing these tasks between the private sector and public financial intelligence units is inherently inefficient. Eliminating the division would address the

problem. In the current system, each individual private party has access to its own client databases 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 databases that financial intelligence units have. Finally, while 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. 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 state financial intelligence units. 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 some difficulty in confirming beneficial owner and controller would remain, 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 to the fact that 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 analysis. Currently the private sector does not have the incentive or the information necessary to do so. The public sector also does not have access to all the private sector-held customer profiling and transaction data that constitutes many of the relevant independent variables. This problem may be obviated if financial intelligence units were tasked with using scientific methods of regression or discriminant analysis and if they had access to 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 could determine the most important parameters, such as likelihood of catching significant criminal proceeds or terrorism financing. Additional benefits of such a system would be avoiding the problems inherent in non-fact based profiling and in turning over to the private sector the secret list of indicators that trigger money laundering and terrorism financing investigations by the public sector.

As will be seen in Part II, keeping these responsibilities in the public sector is essentially the path taken by most tax administrations, thus allowing amalgamation of data from all private sector reporting persons with other confidential data accessible only by the public sector, and permitting the use of statistical analysis to select taxpayers and returns for audit.

There are a few disadvantages to making the system public. First, there could be public opposition based on fears of turning so much private financial data over to a governmental organization. In 1999, privacy concerns were key in defeating a proposed regulation[235] that would have implemented customer identification, account monitoring, and suspicious transaction reporting in the United States, although there was as much concern with banks holding such information with transaction reporting to FinCEN.[236] However, following the terrorist attacks of September 11, 2001 these requirements were spelled out in the USA PATRIOT ACT, which passed easily,[237] and there have been few if any significant complaints voiced in the U.S. Congress since then about such requirements. Turning more financial transaction information over to a governmental agency may spark additional privacy concerns, both in the United States and elsewhere. However, a privacy advantage to such a system would be that private financial institutions and DNFBP would no longer be required to monitor accounts. Additional concerns could be addressed by strengthening, where needed, of data protection rules at financial intelligence units. While tax administrations have access to far less data than would financial intelligence units under such a system, there has been little complaint expressed about privacy concerns in the tax area.

---

235. Know Your Customer, 63 Fed. Reg. 67,524 (proposed Dec. 7, 1998) (withdrawn Mar. 23, 1999).

236. Oliver Ireland & Rachel Howell, *The Fear Factor: Privacy, Fear, and the Changing Hegemony of the American People and the Right to Privacy*, 29 N.C.J. INT'L L. & COM. REG. 671, 677-80 (2004). While a senior staff member of the International Monetary Fund the author of this Article visited the Chief of Staff of an influential Senate Banking Committee member who assured the author that the purpose of the rule was to help the government identify clients who owned guns lay the groundwork for their confiscation.

237. *Id.* at 683.

Another 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 work load, including budget support, increase significantly. It might even be possible to raise financing through a financial institution user fee.[238] 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

As it turns out, certain tax administrations select tax returns for audit in a manner analogous to some of the proposals suggested above for reforming the system of preventive measures. If they can work for income tax they could also work for anti-money laundering and terrorism financing.

Unlike the anti-money laundering system, there is no single global standard for the design and implementation of tax administrations.[239] 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 systems is to improve compliance with revenue laws. While there are many facets to compliance, taxpayer audits are a critical component.[240] In the course of an audit, tax administrations examine a particular taxpayer to determine whether that taxpayer has

238. 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.

239. 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* Gordon, *On the Use and Abuse of Standards for Law*, *supra* note 15, at 584-87, 588-89.

240. OECD, COMPLIANCE RISK MANAGEMENT: AUDIT CASE SELECTION SYSTEMS 5 (2004), *available at* http://www.oecd.org/dataoecd/44/36/33818568.pdf [hereinafter OECD, COMPLIANCE RISK MANAGEMENT].

complied with her or his obligations under the law.[241] A key facet of a tax administration's audit program is the selection of persons for audit.[242] 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 DNFBP 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. 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 have to make any similar judgments. It is the tax administration that makes the decision whether to audit a taxpayer, not the third party.

B. Role of the Private Sector

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

Third party information reporting is a common feature of developed country tax systems.[243] As with information reporting by persons subject to preventive measures for money laundering and terrorism financing, third parties are not compensated for their efforts, making the system another example of an unfunded private mandate.[244] For example, in the United States there is a wide array of third-party information reporting

241. *Id.* at 6.

242. *Id.* at 9.

243. *Id.* at 10-12.

244. Steven A. Dean, *The Incomplete Global Market for Tax Information*, 49 B.C. L. REV. 605, 612-13 (2008) [hereinafter Dean, *The Incomplete Global Market*].

requirements.[245] U.S. payers of wages, interest, or dividend income must report those payments, while brokers must report the amounts realized from securities sales.[246]

As is the case with financial institutions and DNFBP, third party reporters are subject to sanctions for failure to implement their duties.[247] 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 highly 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.[248] There are uncompensated costs associated with such requirements. However, the requirements are relatively straightforward, and third party reporters quickly develop expertise with respect to distilling and disseminating this information.[249] In a manner similar to systems whereby some countries require the automatic reporting of cross-border transactions to financial intelligence units, third party reporting can be easily automated, often by contracting with data management specialists.[250] While taxpayers are also required to report income and deductions and are subject to sanctions for failure to report or for reporting incorrectly, they have a direct interest in fashioning their declarations to minimize their liability; taxpayer sanctions are designed in part to counteract this incentive effect.[251] However, third party reporters have very little direct incentive to misreport in the face of possible sanctions.[252]

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.

---

245. I.R.C. §§ 6050A-6050V (2010)

246. I.R.C. §§ 6041-42 (2010).

247. I.R.C. §§ 6652 (2010).

248. *See, e.g.*, I.R.S. Form W-4 (wages) and I.R.S. Form 1099-Int (interest). There are some exceptions to this general rule. For example, in the United States an employee need not report reimbursements and deduct expenditures for travel and entertainment if the employer's policy tracks the requirements of the Regulations. Treas. Reg. § 1.162-1 (as amended in 1993). In effect, the tax law is applied and enforced by the employer.

249. *See* Jay A. Soled, *Homage to Information Returns*, 27 VA. TAX REV. 371, 373-76 (2007).

250. *See, e.g.*, Totally Paperless, http://www.totallypaperless.com/ (last visited Apr. 4, 2011).

251. Sanjit Dhami & Ali al-Nowaihi, *Why do people pay taxes? Prospect Theory Versus Expected Utility Theory*, 64 J. OF ECON. BEHAVIOR & ORG. 171, 171–92 (2007) (discussing effects of penalties on taxpayer compliance).

252. *See* William L. Burke, *Tax Information Reporting and Compliance in the Cross-Border Context*, 27 VA. TAX REV. 399, 400-01 (2007) (discussing misreporting in the context of third-party estate tax returns).

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 have a specific goal in determining which taxpayers to audit: they generally base their decisions on estimates of the degree of risk of understatement of tax due multiplied by the size of the understatement.[253] In order to implement 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, 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.[254]

The first technique for deciding which returns to audit is third party information return data matching, which is an exception to the "well-kept secret" rule. This is such an effective technique that in the United States, 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, the Internal Revenue Service of the U.S. automatically sends a notice that taxes are due without bothering to go through the audit process first.[255] The Internal Revenue Service has augmented its data-matching by deriving useful additional material from sources other than third-party reporters.[256] In fact, it is because taxpayers are aware that the government is receiving third-party information that they are far less likely to try and cheat with respect to items subject to such reporting.[257]

---

253. *See* information on the U.S., U.K., and France, OECD, Compliance Risk Management, *supra* note 240, at 14-15, 33-34, 45. "The IRS has been traditionally focused on the magnitude of potential audit adjustments." Alex Raskolnikov, *Crime and Punishment in Taxation: Deceit, Deterrence, and the Self-Adjusting Penalty*, 106 COLUM. L. REV. 569, 583-84 (2006).

254. Raskolnikov, *supra* note 253, at 583.

255. Jeffrey A. Dubin, Michael A. Graetz, & Louis L. Wilde, *The Changing Face of Tax Enforcement, 1978-1988*, 43 TAX LAW. 893, 901 (1989-1990) [hereinafter Dubin *et al*., *The Changing Face*].

256. For example, data on dependents (which can result in deductions from income) are obtained from various government sources. *See* 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).

257. Leandra Lederman, *Statutory Speed Bumps: The Roles Third Parties Play in Tax Compliance*, 60 STAN. L. REV. 695, 697 (2007); James Alm, John Deskins & Michael McKee, *Third-Party Income Reporting and Income Tax Compliance* 2-3 (Andrew Young School of Policy Studies, Working Paper No. 06-35, 2006), *available at* http://aysps.gsu.edu/publications/2006/index.htm.

The next technique is the use of algorithms such as discriminant or regression analysis, the gold standard for determining the statistical relationship between dependent and independent variables and one not used by any party in the preventive measures system. The Organization for Economic Cooperation and Development has identified the United States and the United Kingdom as using such systems.[258] The U.S. system uses a discriminant function analysis.[259] According to the Internal Revenue Service, 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. Internal Revenue Service personnel then screen the highest-scoring returns, "selecting some for audit and identifying the items on these returns that are most likely to need review." [260] While the Internal Revenue Service has admitted to using such a system, the process of the analysis is "one of the best kept secrets in government." [261] Prior to the institution of the DIF system, about half of all Internal Revenue Service 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).[262]

Because the government enforces strict secrecy over the details of the DIF system, 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 hypothesis sufficient data must first be collected. Beginning in 1963, such data was collected through the Taxpayer Compliance Measurement Program, whereby the Internal Revenue Service undertook thorough audits of representative samples of individual income tax returns approximately every three years.[263] This program of data collection was abandoned because of the burden placed on those taxpayers who had the bad luck to be selected for audit,[264] but it has been replaced with National Research

258. OECD, COMPLIANCE RISK MANAGEMENT, *supra* note 240, at 14-15, 34-35.

259. IRS, *The Examination (Audit) Process* (2006), http://www.irs.gov/newsroom/article/0,,id=151888,00.html [hereinafter IRS, Examination (Audit) Process].

260. *Id.*

261. Dubin *et al.*, *The Changing Face*, *supra* note 255, at 900.

262. Robert E. Brown & Mark J. Mazur, *The National Research Program: Measuring Taxpayer Compliance Comprehensively*, 51 KAN. L. REV. 1255, 1261-62 (2003) [hereinafter Brown & Mazur, *The National Research Program*].

263. *Id.* at 1261-62.

264. *Id.* at 1263.

Program, a data collection program that relies on audit information as well as added data obtained from various confidential government sources and public records (e.g., current and prior addresses, real estate holdings, business registrations, and corporate records).[265] Obviously, while limited, this system is far 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, it appears that the number of independent variables is limited. At least in part for this reason, the Internal Revenue Service does not rely solely on discriminant function analysis to select returns for audit. Like financial institutions and DNFBP, the Internal Revenue Service, as well as many other developed country tax administrations,[266] uses more subjective "red flag" types of reviews.[267] 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.[268]

Apparently in order to make red flag application more standardized and automated, the Internal Revenue Service has developed the 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 have been included, but the Internal Revenue Service stated that it was working to expand the number.[269] The U.S. also uses other far more general criteria to determine audits.

Given the opportunity to collect more underpaid taxes from fewer audits, in advanced jurisdictions like the United States tax authorities audit

265. IRS, REDUCING THE FEDERAL TAX GAP: A REPORT ON IMPROVING VOLUNTARY COMPLIANCE 7 (2007), *available at* http://www.irs.gov/pub/irs-news/tax_gap _report_final_080207_linked.pdf; Brown & Mazur, *The National Research Program*, *supra* note 262, at 1264-86; Nina E. Olson, *supra* note 256, at 9.

266. Including Canada, the U.K. and France. OECD, COMPLIANCE RISK MANAGEMENT, *supra* note 240, at 25-26, 34-35, 45.

267. Raskolnikov, *Crime and Punishment in Taxation*, *supra* note 253, at 587-94.

268. An indication of "red flags" are items required in Schedule M-1 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. *Id.* at 585. "Even less information is required of an unincorporated sole proprietor on Schedule C to Form 1040." Ronald A. Pearlman, *Demystifying Disclosure: First Steps*, 55 TAX L. REV. 289, 296 (2002). Interestingly, this data is not filed by third 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.

269. OECD, COMPLIANCE RISK MANAGEMENT, *supra* note 240, at 15-17.

returns of higher income persons more often than those of lower income. Also, individuals with wage income only, which is subject to third party information reporting, and who do not itemize deductions are also audited at a lower rate.[270] This system appears to be far more objective and efficient than the more subjective red flag systems used by both financial institutions and DNFBP and financial intelligence units to spot suspicious transactions.

It is unknown exactly why the Internal Revenue Service has not expanded its discriminant function system to include more independent variables, but it may have something to do with the additional expense involved and the lack of support for additional funding for the Internal Revenue Service.[271]

D. 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 proposition that such an "objective information" rule be exported to that system. By turning all analytical tasks over 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. Finally, there is no inherent contradiction between developing an effective system for audit selection and keeping such a system out of the hands of possible tax cheats: no private sector person is involved in audit selection.

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 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

270. Raskolnikov, *Crime and Punishment in Taxation*, *supra* note 253, at 583-84.

271. Confidential Interview, I.R.S. District Director, in Cambridge, Mass. (May 1, 1994).

into many entities. This is clearly an advantage over the preventive measures system.

Another major advantage is that the statistically-based techniques used to select returns for audit are kept as secret as possible from the public, making it harder for the private sector to develop techniques that would avoid triggering an audit. 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. By requiring financial institutions and DNFBP to design and implement requirements that are poorly described, expensive, and unfunded, the FATF Recommendations invite failure. Given that the private sector's main motive is profit, one would reasonably predict that it would seek to reduce costs by spending as little as possible on implementing those requirements. Because of the Recommendations' subjective nature, it is possible for the private sector to define downward its duties without fear of sanction. In addition, the requirements describe a mandate that the private sector has little objective capacity to implement, even if it wanted to.

A rethought system would eliminate all but the most objective and least expensive unfunded private sector mandates. Specifically, private sector persons currently tasked with client identification, profiling, record-keeping, monitoring, and suspicious transaction reporting would be required to perform only the first two tasks. Added to this would be a requirement to transmit certain profiling information and all financial transactions. 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 of any kind, domestic or international, perhaps in excess of a certain de minimis limit. All data would, where possible, be transmitted electronically.

All other aspects of the preventive measures system would be allocated to the government. This would eliminate the current private-sector cost-savings disincentive effects in the current system. The current system requires the government to examine reports from the private sector and determine which of those reports should be further investigated; in

effect, to determine which "suspicious" reports are *really* suspicious. Dividing the search for the suspicious and the really suspicious between the private sector and public financial intelligence units seems inherently inefficient. Because the government has far greater access to important data, it would also vastly increase the capacity of the system to design and implement an effective system for identifying likely criminals and terrorists.

Specifically, financial intelligence units would be tasked with analyzing data 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 the probability of laundering multiplied by magnitude of laundering. With respect to terrorism finance, this could be the probability of financing or some formula of probability multiplied by the potential danger that such financing might cause. As is now the case, financial intelligence units would be required to send such reports on to law enforcement for investigation. Strict data protection and secrecy laws would continue to apply to the financial intelligence unit.

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. Because of the resources and time required for such empirical and statistical analysis, this 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 Internal Revenue Service's Dependent Data-based System. All information concerning data analysis and would be kept strictly secret from the public, including financial institutions and DNFBP.

Some problems could still persist. Government bureaucracies are often inefficient, and financial intelligence units may have difficulty implementing their expanded roles. There may also be political pushback because of the greater costs to the public sector budget, or because of a perception that the government's greater authority could be a threat to

individual freedom. But the improvements in catching criminals and terrorists in a rethought system should outweigh these potential downsides.

CONCLUSION

The current system designed to prevent money laundering and terrorism financing does not work well. It is based on a faulty theoretical construction. The FATF Recommendations require financial institutions to design and implement requirements to monitor client transactions and report those that raise suspicion of money laundering or terrorism financing. However, because these requirements are poorly described, expensive, and unfunded, the FATF Recommendations invite failure. Because of their subjective nature, it is possible for the private sector to define downward its costly duties without fear of sanction. In addition, private sector financial institutions do not have sufficient expertise or data to design and implement such systems even if they wished to

The current system also requires the government to examine reports from the private sector and determine which of those reports should be further investigated; in effect, to determine which "suspicious" reports are *really* suspicious. Dividing these tasks between the private sector and public financial intelligence units is 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). Finally, it introduces an inherent contradiction: the public sector is tasked with informing the private sector how best to detect launderers and terrorists, but to do so could act as a road map on how to avoid detection should such information fall into the wrong hands.

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 tax administrations select taxpayers for audit investigation. Also, there should be significant overall 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 treasury, because this would in part finance greater governmental anti-terrorism work, the added public sector costs might be politically acceptable.