Penn State International Law Review

Volume 26
Number 1 *Penn State International Law Review*

Article 3

7-1-2007

Smarter Smart Sanctions

Peter L. Fitzgerald

Smarter "Smart" Sanctions

Peter L. Fitzgerald*

I. Introduction

Targeted or "smart" sanctions are still pretty dumb. Governments need to do more to design their sanctions programs with commercial practicality in mind, and businesses and others in the regulated community need to work more closely with government to ensure that these programs are workable and capable of achieving their stated objectives.

Economic and financial sanctions, whether aimed at countries such as Iran or North Korea or more amorphous targets like weapons proliferators, narco-traffickers, and global terrorists, are increasingly important tools for governments attempting to address some of the more intractable international issues of the late 20th and early 21st centuries. However, sanctions are also an example of the sort of regulatory program where achieving governmental policy objectives depends more upon voluntary compliance than upon actual governmental enforcement. Nevertheless, as documented by the recent British House of Lords Economic Affairs Committee's *Inquiry into the Impact of Targeted Sanctions,*[1] the Swedish Institute of International Law's *Report to the Swedish Foreign Office on Legal Safeguards and Targeted Sanctions* in 2002,[2] and the congressionally created Judicial Review Commission on Foreign Asset Control's *Final Report to Congress* in 2001,[3] the

---

* © Peter L. Fitzgerald; Professor of Law; Stetson University College of Law; Gulfport, Florida. This paper was adapted from Written Evidence initially prepared for the British House of Lords Economic Affairs Committee, and portions of the text are included in House of Lords Economic Affairs Committee, THE IMPACT OF ECONOMIC SANCTIONS, VOL. II: EVIDENCE, Second Report of Session (HL Paper 96-II) (2007), at 149.

1. House of Lords Economic Affairs Committee, THE IMPACT OF ECONOMIC SANCTIONS, Second Report of Session (HL Paper 96-II) (2007).

2. Iain Cameron, Swedish Institute of International Law, REPORT TO THE SWEDISH FOREIGN OFFICE ON LEGAL SAFEGUARDS AND TARGETED SANCTIONS, (OCTOBER 2002) *available at* http://resources.jur.uu.se/repository/5/PDF/staff/sanctions.pdf.

3. Judicial Review Commission on Foreign Asset Control, FINAL REPORT TO CONGRESS (January 2001). The congressionally created Judicial Review Commission on

governmental blacklisting of particular entities or individuals that lies at the heart of what are now called "smart" or "targeted" sanctions programs is beset with numerous issues that undermine compliance and impacts the perceived legitimacy of these programs. Uncertainty regarding the details of the controls, the obligations they impose, and the manner of their enforcement, is the single greatest impediment to the types of commercially practicable sanctions that would lead to more widespread voluntary compliance.

There are five principal areas of uncertainty associated with the sanctions as currently formulated and administered. These can be seen most clearly by focusing upon the anti-terrorist sanctions programs.

II. The Compliance Issues Posed by Smart Sanctions

A. Uncertainty as to Who Comprises the "Regulated Community" that Must Comply with the Sanctions

At their core, economic sanctions are controls that are directed primarily at, and implemented by, banks and financial institutions.[4] However, reflecting their origins as foreign policy tools, sanctions programs are often written in broad terms that impose compliance

---

Foreign Asset Control prepared the most comprehensive review of U.S. economic sanctions programs since the examination of the WWII era controls conducted in 1947. The Commission was established by Congress as part of a legislative compromise when it passed the Foreign Narcotics Kingpin Designation Act, because of concerns over the due process issues associated with the blacklisting mechanisms in the various U.S. economic sanctions programs. Chaired by Larry D. Thompson, prior to his becoming Deputy Attorney General in the Bush Administration, the Commission conducted a year long $1 million study of the sanctions programs administered by the Treasury Department's Office of Foreign Assets Control ("OFAC"). The Commission's Final Report to Congress was submitted to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence on January 23, 2001. The House Committee on International Relations, House Committee on the Judiciary, Senate Committee on Foreign Relations and Senate Committee on the Judiciary also received copies. The Report, and its accompanying appendices, totals approximately 1900 pages. While only a few hard copies were printed, the Report is available in microfiche at selected Federal Depository Libraries under SuDoc. Y 3.2:F 76/F 49; Y 3.2:F 76/F 49/V.1-2; GPO Item No. 1089 (MF) and it is also available online at http://www.law.stetson.edu/JudicialReviewCommission/.

4. As stated by the general counsel of the U.S. Treasury Department in his testimony before the Senate Judiciary Subcommittee on Terrorism, Technology and Homeland Security, with particular regard to the anti-terrorist sanctions:

> [t]his is a profoundly uncommon war. . . . It is shadow warfare. The primary source of the stealth and mobility necessary to wage it is money. It is the fuel for the enterprise of terror. . . . If we stop the money, we stop the killing.

Written Testimony of David D. Aufhauser General Counsel, Department of the Treasury before the Judiciary Subcommittee on Terrorism, Technology and Homeland Security, June 26, 2003, *available at* http://www.treasury.gov/press/releases/reports/js5071.pdf.

obligations on those both within and without the financial community, and for all transactions with blacklisted parties, involving even the smallest amount or account.[5]

From the perspective of those who must comply with the controls, however, this creates uncertainty as to the scope of one's compliance obligations. In the United States this is sometimes called the "McDonald's problem."[6] Is a fast-food retailer obligated to establish a compliance process for all its cash hamburger sales to ensure that it does not engage in a transaction with Osama bin Laden or one of the other individuals or entities found on a governmental blacklist? Put differently, is it sound policy to require those outside the financial community to choose between establishing expensive internal compliance processes for all of their operations irrespective of the risks posed under the circumstances or, alternatively, to rely upon prosecutorial discretion in the event a technically prohibited transaction occurs?

Ironically, the result of broadly written controls is not wider compliance. Rather, those outside of the financial institutions at the core of the controls, recognizing that governmental enforcement resources are limited, may not engage in a high degree of "voluntary" compliance with what they perceive to be commercially impractical requirements. The government then loses the leverage that broader compliance would offer in achieving governmental policy objectives.[7]

---

5. The governmental blacklisting of particular entities and individuals was historically used as a secondary tool to augment a primary economic embargo directed at particular geographic enemy, often as an adjunct to actual hostilities. *See* P.L. Fitzgerald, *Managing "Smart Sanctions" Against Terrorism Wisely*, 36 NEW ENGLAND L. R. 957, 980 (2002). Over the past several decades blacklisting shifted from being a secondary tool incidental to actual or economic warfare against another state, to become a primary tool whereby governments sought to lead or alternatively coerce other nations into different actions as a foreign policy matter, or to distance a country and its nationals from other states engaged in undesirable behavior. *See* P.L. Fitzgerald, *"If Property Rights Were Treated Like Human Rights, They Could Never Get Away With This": Blacklisting and Due Process in U.S. Economic Sanctions Programs,* 51 HAST. L.J. 73, 89-90 (1999).

6. *See e.g.,* Statement Of Donald Ray Looper Before The Judicial Review Commission on Foreign Asset Control (September 22, 2000) in Judicial Review Commission on Foreign Asset Control, APPENDICES TO THE FINAL REPORT TO CONGRESS (January 2001), Vol. 1, Appendix E—Written Submissions from Witnesses Who Testified, 172, at 179, *available at* http://www.law.stetson.edu/JudicialReviewCommission/frtcappendicesvolume1_E.pdf.

7. Achieving broader compliance that reaches outside of the financial industry that typically comprises the regulated community for economic sanctions programs is particularly important in the anti-terrorist sanctions. As the U.S. Treasury Department counsel Aufhauser also noted:

> [t]errorist financing is a unique form of financial crime. Unlike money laundering, which is finding dirty money that is trying to hide; terrorist financing is often clean money being used for lethal purposes. . . . Terrorists

Given the importance of the objectives behind targeted sanctions, governments need to move beyond the mere political statement made by adding names to a blacklist and create a system where the controls triggered by the act of blacklisting are more effective. The former general counsel for the U.S. Treasury Department, David Aufhauser, noted that "both terrorist financing and traditional financial crimes have one thing in common—they leave a financial footprint that allows us to trace financial flows, unravel terrorist financing networks, and uncover terrorist sleeper cells."[8] Unlike much of the other evidence gathered relating to terrorism, which can be "suspect, the product of interrogation, rewards, betrayals, deceits . . . a financial record doesn't lie."[9] The U.S. Secretary of the Treasury, Henry M. Paulson Jr. recently noted:

> [t]he starting point for Treasury's approach to targeted financial measures is information. To identify and act against threats, we need specific, current, and reliable intelligence. And the global financial system is a rich source of the information we need. . . . In 2004,

---

> have also used informal value transfer systems such as hawala as a means of terrorist financing. The word "hawala" (meaning "trust") refers to a fast and cost-effective method for the worldwide remittance of money or value, particularly for persons who may be outside the reach of the traditional financial sector. . . . The United States has already taken steps to regulate hawalas and informal value transfer systems. The PATRIOT Act requires money remitters (informal or otherwise) to register as "money services businesses" or "MSBs," thereby subjecting them to existing money laundering and terrorist financing regulations, including customer identification, record keeping and suspicious transaction reporting requirements. Well over 14,000 money service businesses have registered with the federal government and are now required to report suspicious activities. In order to increase awareness within the diverse MSB community nationwide about their obligations under the MSB rules, FinCEN plans to conduct an outreach campaign to include advertising, community outreach and the distribution of educational materials.

Written Testimony of David D. Aufhauser General Counsel, Department of the Treasury before the Judiciary Subcommittee on Terrorism, Technology and Homeland Security, June 26, 2003, *available at* http://www.treasury.gov/press/releases/reports/js5071.pdf.

8. *Id.*

9. The Treasury Department General Counsel continued to state that financial records are:

> enormously useful—helping to identify, locate and capture bad guys, mapping out a network of connections that tie an anonymous banker to a suicide bomber, helping to evaluate the credibility and immediacy of a threat, and preventing a calamity by starving the enterprise of terror of its fuel. . . . I [once believed] that a dollar well deployed could enhance opportunity and thereby diminish antipathy to our values. But I now know that preventing a dollar from being misapplied can be of equal service and is, perhaps, the surest weapon we have to make the homeland secure and to let our kids go to schools that teach tolerance and respect for people of all faiths.

Oral Testimony of David D. Aufhauser General Counsel, Department of the Treasury before the Judiciary Subcommittee on Terrorism, Technology and Homeland Security, June 26, 2003, *available at* http://www.treasury.gov/press/releases/js507.htm.

> Treasury became the first finance ministry in the world to develop in-house intelligence and analytic expertise to use this information. We now work with the broader intelligence community, requesting the data necessary to understand the financial networks that threaten our national security. Treasury then evaluates this information with an eye towards potential action—be it a designation, an advisory to the private sector, or a conversation to alert other finance ministers to a particular threat or bad actor.[10]

Thus, well-crafted economic sanctions can serve as an important tool in gathering the intelligence necessary to deal with threats like global terrorism and weapons proliferation in addition to simply blocking targeted parties' access to their assets.

The "leakage" from economic sanction programs that was acceptable when the controls were only a secondary foreign policy tool directed against a foreign state should no longer be tolerable when the objective is preventing actual acts of terrorism or gathering the information necessary to prosecute those who commit such acts. Accordingly, governments need to identify more precisely who should comply with their controls, using a risk based analysis, and then collaborate with that regulated community in creating economic sanctions that are commercially practical and enforceable in order to enhance compliance. As is done in many other financial regulatory programs, this is an approach that adjusts compliance obligations based upon the size and nature of the institution involved, its market, products and services, and the likelihood of encountering those parties targeted by the sanctions program.

B. Uncertainty as to the Targets of Targeted Sanctions

Providing accurate information precisely identifying a particular party or entity as a sanctions target is often difficult, but is nevertheless crucial for an efficient screening system for any business seeking to determine which transactions should be controlled or assets blocked or frozen. Blacklists are inherently both under- and over-inclusive. For example, while "Usama Bin Ladin" was blacklisted in the United States as early as August 22, 1998, "Osama bin Laden" did not appear on the list until after the 9/11 attacks.[11] Similarly, following the attacks in 2001, the United Nations, European Union, and the Bank of England added

10. U.S. Treasury Dept., Press Release HP-457, *Remarks by Treasury Secretary Paulson on Targeted Financial Measures to Protect Our National Security* (June 14, 2007) *available at* http://www.ustreas.gov/press/releases/hp457.htm.

11. *See* P.L. Fitzgerald, *Managing Smart Sanctions Against Terrorism Wisely*, *supra* note 5, at 968-69.

"Osama bin Laden" to their blacklists under a number of aliases and variations. However, even today neither the U.N. Consolidated List, nor the Bank of England's list, show the alternate spelling of "bin Ladin."[12]

If a precise match with a government blacklist is required, targeted individuals and entities might escape the controls due to minor variations in the names. Conversely, if not enough rigor is applied in the matching process, a blacklist screening system can easily be overwhelmed by the number of false matches. A similar issue arises when common names appear on the blacklist, generating a large number of unintended matches. For example, under the old Yugoslav sanctions programs the common but indefinite name "Global" was found on the blacklist without any further identifying information.[13] In the recent past, press reports have indicated that prominent figures such as Senator Ted Kennedy or the President of Bolivia, or even children, were erroneously stopped at airports because of the similarity between their names and those appearing on the U.S. terrorist "no fly" blacklist.[14] These types of problems are further exacerbated when the names of those individuals and entities targeted by the blacklist have multiple spellings or are being transliterated. For example, the Arabic "محمد" may be transliterated as Muhammad, Mohammad, Mohammed, Mohamed, Muhammed, Mahommed, Mehmed, Mehmet, and Mahomet; and many other common Arabic or foreign names that appear among the current sanctions blacklist entries may similarly appear in multiple forms or spellings.[15]

While government authorities have tried to address these problems in many of the newer blacklist entries by providing more specific information regarding the targeted parties, many of the old entries (*e.g.* the original U.N. Taliban lists) remain without any unique identifiers. As there are more than six thousand different parties or entities found on the various governmental blacklists, all of which must be incorporated into a company's internal compliance and screening programs, matching

12. *See* U.N. Consolidated List of Individuals And Entities Belonging to or associated with the Taliban and Al-Qaida Organization as Established and Maintained by the 1267 Committee, *available at* http://www.un.org/Docs/sc/committees/1267/tablelist.htm; Bank of England Consolidated List of Financial Sanctions Targets (Full List), *available at* http://www.bankofengland.co.uk/publications/financialsanctions/sanctionsconlist.htm.

13. *See* P.L. Fitzgerald *"If Property Rights Were Treated Like Human Rights, They Could Never Get Away With This"* . . ., *supra* note 5, at 123.

14. *See e.g.*, Steve Kroft, *Unlikely Terrorists on No Fly List,* CBS 60 Minutes, (June 7, 2007) *available at* http://www.cbsnews.com/stories/2006/10/05/60minutes/main2066624.shtml.

15. *See* Brian Whitaker, *Lost in Translation,* The Guardian Unlimited (June 10, 2002) *available at* http://www.guardian.co.uk/elsewhere/journalist/story/0,7792,730805,00.html; *see also* http://en.wikipedia.org/wiki/Muhammad_%28disambiguation%29.

accounts and customers to the blacklist entries poses significant problems.

What should be done with a transaction in London involving "Mohammed Salah," for example? Shortly after the attacks in 2001, the U.N. blacklisted "Muhammad Salah (individual) (a.k.a. Nasr Fahmi Nasr Hasanayn)" as part of its Al Qaida and Taliban sanctions,[16] and the E.U. added the same entry in 2002.[17] In 2004, the U.N. and the E.U. both updated their blacklist information to indicate that "Muhammad Salah" was in fact an alias for "Nasr Fahmi Nasr Hassannein" or perhaps "Naser Fahmi Naser Hussein," and added that the target was born on October 30, 1962, in Cairo.[18] All of this is reflected on the Bank of England's Consolidated List,[19] but the blacklist maintained by the U.S. Treasury Department's Office of Foreign Asset Control only shows the more limited original information from 2001.[20] However, the U.S. does have another "specially designated terrorist" blacklist entry, related to its sanctions on those who threaten the Middle East peace process, which reads:

> SALAH, Mohammad Abd El-Hamid Khalil (a.k.a. AHMAD, Abu; a.k.a. AHMED, Abu; a.k.a. SALAH, Mohammad Abdel Hamid Halil; a.k.a. SALAH, Muhammad A.), 9229 South Thomas, Bridgeview, IL 60455; P.O. Box 2578, Bridgeview, IL 60455; P.O. Box 2616, Bridgeview, IL 60455-661; Israel; DOB 5/30/53; Passport 024296248 (United States); SSN 342-52-7612 (individual) [SDT].[21]

The name "Mohammed Salah" does not precisely match any of these entries, irrespective of the varying amounts of detail provided by the different blacklisting authorities. A business struggling with complying

16. Press Release, Security Council, Security Council Committee Concerning Afghanistan Issues List Pursuant To Paragraph 8(C) Of Resolution 1333 (2000),_U.N. Doc._AFG/150 SC/7166 (Oct. 8, 2001), *available at* http://www.un.org/News/Press/docs/2001/afg150.doc.htm.

17. Council Regulation (EC) No 881/2002 of 27 May 2002, *available at* http://eur-lex.europa.eu/lexuriserv/site/en/oj/2002/l_139/l_13920020529en00090022.pdf.

18. Press Release, Security Council, Security Council Committee Approves Correction Of Identifying Information Of Fifty-Three Individuals, Ten Entities On Consolidated List, U.N. Doc. SC/8259 (Dec. 12, 2004), *available at* http://www.un.org/News/Press/docs/2004/sc8259.doc.htm; Commission Regulation (EC) No 2145/2004 of 15 December 2004, *available at* http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2004/l_370/l_37020041217en00060016.pdf.

19. *See* Consolidated List Of Financial Sanctions Targets In The UK, *available at* http://www.bankofengland.co.uk/publications/financialsanctions/sanctionsconlist.htm.

20. *See* Office of Foreign Assets Controls, Specially Designated and Blocked Nationals List, *available at* http://www.ustreas.gov/offices/enforcement/ofac/sdn/t11sdn.pdf.

21. *See id.* This Specially Designated Terrorist list dates to the 1995 blacklisting of those who threatened the Middle East peace process. *See* http://www.treasury.gov/offices/enforcement/ofac/sdn/sdnew95.txt.

with the controls may have more information which would help it determine if a match with one of the blacklist entries has occurred, depending upon the nature of the transaction and the degree to which a particular type of business really "knows its customers." But if not, how much additional information must it demand from its customer in order to meet its compliance obligations before it can proceed? Clearly, if the individual subsequently turned out to be either the 43 year old Egyptian-born Al Qaida supporter or the 53 year old American national targeted by the U.S. sanctions, the minor difference in the spelling would be an indefensible distinction in either the political realm or in the marketplace of public opinion. Transactions involving the true targets of the sanctions need to be identified and addressed, while minimizing the impact on dealings with those who are not the actual targets of the sanctions programs.

Thus, in addition to structuring the sanctions programs' controls to impose the greatest compliance obligations on a risk-based model, there also needs to be some official avenue for those with the legal compliance burden to definitively determine whether the party with whom they are dealing is or is not a sanctions target, and also to resolve conflicts or differences among the various governmental blacklists. Moreover, in order to be commercially practicable, this needs to be both an expeditious and reliable process. The absence of such a communication process between regulators and the regulated community is perhaps the single most significant compliance issue affecting the current sanctions programs.

C. Uncertainty Regarding Liability

In a risk-based controls system businesses should not expect to face an enforcement action for every failure to identify or block a transaction with a blacklisted party. Standards for what constitutes an acceptable level of compliance are needed, adjusted for the industry involved and the risks presented.[22] While a customer or account based screening system may be appropriate for banking institutions, non-bank money transmitters often do not have customer accounts. For example, money orders can be issued for a low face value by a convenience store to a

22. For a number of suggestions as to how such an approach could be implemented across different elements of the financial community refer to the various industry responses submitted to the U.S. Treasury Department when it issued a request for comments regarding its new enforcement practices in early 1996. *See* U.S. Treasury Dept., Office of Foreign Assets Controls *Economic Sanctions Enforcement Procedures for Certain Banking Institutions*, 71 Fed. Reg. 1971 (Jan. 12, 2006), and the record of comments available at http://www.ustreas.gov/offices/enforcement/ofac/interim/enf_guide/enf_comments.pdf.

retail customer who may not provide a name. Even when larger non-bank funds transmitters such as Western Union or American Express request the names of a sender and a recipient, they may not engage in extensive verification of their customers' or recipients' identities. While these different businesses may all belong to the core regulated community for sanctions purposes, the risks posed and the standards of what constitutes an acceptable level of compliance for each might well vary. If governments are unwilling or unable to promulgate appropriately differentiated compliance standards themselves, regulators should be prepared to recognize "best practices" for compliance developed by the various private industries comprising the regulated community.

Arriving at standards for an acceptable level of compliance is especially important with regard to the "interdiction software" many companies use to automatically screen their operations against blacklist entries. For example, to what degree should the software employ fuzzy logic, or a variable level of matching, to address whether a name like "Mohammed Salah" or "Global" matches governmental blacklist entries?

Even with the best automated programs some transactions will slip through the screening process. The Bank of America noted in correspondence with the U.S. Treasury Department's Office of Foreign Assets Control that:

> [l]arge banking institutions handle millions of transactions each day and, despite state of the art interdiction systems, frequent staff training and the institution's best efforts, it is statistically inevitable that a large bank will have inadvertent violations of [the] sanctions. Inadvertent violations that do not evidence a systemic weakness in an institution's . . . compliance program should not result in penalty proceedings, nor should inadvertent violations in the past be used to classify a large banking institution as a "repeat offender."[23]

Conversely, small institutions, who lack the resources and in-house expertise of a Bank of America to handle their own screening operations, should be permitted to outsource their compliance systems to larger institutions or specialized firms, and rely upon the expertise of those running these outsourced systems rather than being held to the current strict liability standard.

Standards for acceptable levels of compliance should also encompass situations where "after the fact" blacklist screening may be more commercially practicable or appropriate than the real-time

23. *See* Letter from Bank of America Legal Department, to U.S. Treasury Dept. Office of Foreign Asset Controls, (Feb. 7, 2006), *available at* http://www.ustreas.gov/offices/enforcement/ofac/interim/enf_guide/enf_comments.pdf.

screening often urged by regulators. Real-time screening may not be practical for a McDonalds-like or low value automated transaction conducted at "internet speed," particularly if there are questions about a potential match.[24] Many industries assert that, in some circumstances, "after the fact" blacklist screening can be as useful in meeting government objectives as real-time screening. Accepting a deposit to open a new account, for example, and then screening that account customer against the blacklist as part of an overnight batch process would result in the target's funds being blocked rather than being turned away. Such a process also serves governmental identification, tracking, and evidentiary objectives that would not be met if the transaction was refused under a real-time screening system. Real-time blacklist screening may also place a teller or similar individual in harm's way if it requires informing the person attempting to open the account why the transaction is being refused.

Lastly, once these standards for acceptable compliance are established, they should be accompanied by "safe-harbors" from liability for those who comply with the standards, even where an innocent or technical violation of the sanctions has occurred. This is consistent with a variety of other banking laws.[25] A different sort of "safe-harbor," which clearly and expressly insulates the regulated community from liability to its customers or account holders for freezing their accounts or disrupting their transactions would also be a useful addition to many sanctions laws or regulations.

D. *Uncertainty Regarding How to Handle Mistakes or Challenges to Targeted Sanctions*

Mistakes are inevitably made in any blacklisting process, but often there is no express right for an affected party to know the basis of the blacklisting decision or to have an independent review of the government's actions. Even in the absence of a mistake, circumstances may change over time such that a blacklisted party may wish to challenge the basis for its ongoing designation. A meaningful right of

24. *See generally*, P.L. Fitzgerald, *Hidden Dangers in the E-Commerce Data Mine: Governmental Customer and Trading Partner Screening Requirements*, 35 INT'L LAW 47 (2001).

25. *See e.g.* Sections 313 and 319 of the USA PATRIOT ACT and 31 C.F.R. 103.177(b). U.S. law and regulations requires financial institutions to gather a variety of information from their correspondent accounts, and prohibit maintaining correspondent accounts with "shell banks." However, a "safe-harbor" was provided to those institutions who obtain certain "certifications" from their foreign correspondents, in recognition of the difficulty of the burden in gathering this information from a large number of institutions, and the difficulty in determining whether a foreign bank is a "shell bank."

review of these blacklisting decisions is especially important as the number of blacklisted parties grows, along with the number of governments promulgating these lists. Many of these sanctions programs, including those in the U.S., fail to provide an express right for the affected party to know the basis for a blacklisting decision. While this certainly protects sensitive information, it also creates huge practical hurdles for any affected party seeking to correct mistakes or otherwise challenge the government's actions.[26]

Entirely apart from situations where the match between an account or customer with a blacklist entry is questionable, there will be cases where the propriety of the blacklisting of a properly identified party is at issue. One notable example involves the Bank of America's blocking assets worth $24 million that belonged to the Saudi Arabian businessman, Salah Idris, in 1998. This action followed the U.S. bombing of two of Osama bin Laden's camps in Afghanistan, along with Idris's pharmaceutical plant in Sudan, in retaliation for the terrorist attacks on the U.S. Embassies in Kenya and Tanzania. Idris denied any links to Osama bin Laden, and sued the U.S. government for defamation and compensation. Rather than defend the lawsuit Idris's assets were voluntarily "unblocked."[27] Although the U.S. government asserted that the unblocking was prompted by concerns over exposing intelligence sources if it answered the lawsuit, much of the public basis for the government's actions regarding Idris and his El Shifa pharmaceutical plant was subsequently discredited.[28]

Another example involves Maher Arar, a Syrian born Canadian software engineer, detained by American officials in 2002 while transiting the U.S. on his way back to Canada following a trip to Tunis. Arar was stopped and then deported to Syria, where he was held for more

26. As initially promulgated in 1998 OFAC's Reporting and Procedures Regulations (RPR) provided that those seeking administrative reconsideration of their blacklisting could review the factual basis for the agency's actions, although sensitive material could be redacted. 31 C.F.R. § 501.807 (1998). However, less than a year later, OFAC withdrew the ability to obtain this material without explanation. *See* U.S. Treasury Dept, Office of Foreign Assets Controls, *Reporting and Procedures Regulation: Procedure for Requests for Removal from List of Blocked Persons, Specially Designated Nationals, Specially Designated Terrorists, Foreign Terrorist Organizations, Specifically Designated Narcotics Traffickers, and Blocked Vessels,* 64 Fed. Reg. 5,614 (Feb. 4, 1999). Parties may still request that a blacklisting decision be administratively reconsidered, but they no longer have a regulatory right to review the basis for the agency's actions. *See* 31 C.F.R. § 501.807 (2005).

27. *See* P.L. Fitzgerald, *Managing "Smart Sanctions" Against Terrorism Wisely*, *supra* note 5, at 976-78.

28. *See* Doug Bandow, *Making it Right in Sudan; U.S. Owes Damages For Pharmaceutical Bombing*, WASH. TIMES, Aug. 10, 2001, at A21. However, Idris has yet to receive any compensation.

than a year and tortured, on the basis of what was later determined to be false accusations of terrorist involvement provided by Canadian police. In 2006, the Canadian Prime Minister apologized and the government paid $10 million (cdn) to settle Arar's civil suit in Canada, but his name still remains on the U.S. border watchlist.[29]

In comparison to the substantive and procedural safeguards commonly found surrounding the imposition of penalties and the deprivation of property in civil or criminal proceedings, there is very little oversight or judicial review exercised when these same sorts of governmental actions are styled as "foreign policy" measures as part of a sanctions program. Even when cases get to court, doctrines regarding standing to file a lawsuit, the scope of judicial review and deference to executive authority, along with the traditional notion that blocking or freezing actions are "temporary" foreign policy measures, effectively preclude a substantive challenge to most governmental blacklisting actions.[30] An extensive review of these issues prompted the congressionally created Judicial Review Commission on Foreign Assets Control to focus seven of its twelve recommendations to the U.S. House and Senate Intelligence Committees on the need for more due process protections in the administration of the various U.S. economic sanctions programs.[31]

The situation in Europe is not significantly different. Sanctions continue to be regarded as foreign policy measures largely exempt from judicial or administrative review. For example, three Somali-born Swedish nationals Abdi Abdulaziz, Abdirisak Aden, and Ahmed Ali Yusuf, all employees of the Al Barakaat International Foundation branch in Stockholm, were blacklisted and their assets frozen pursuant to Regulation (EC) 2199/2001 on November 12, 2001.[32] Their names were included on the European blacklist because they had been added to the U.N. Security Council blacklist on November 9, 2001, after first appearing on the U.S. blacklist as part of the Taliban and Al Qaida sanctions two days earlier.[33] Although it froze the assets, Sweden also

29. *See* Ian Austen, *Canada Will Pay $9.75 Million to Man Sent to Syria and Tortured,* N.Y. TIMES, Jan. 27, 2007, at A5.

30. *See generally* P.L. Fitzgerald, *Drug Kingpins and Blacklisting: Compliance Issues with U.S. Economic Sanction (Part 1)*, 4 J. MONEY LAUNDERING CONTROL 360 (2001); P.L. Fitzgerald, *Drug Kingpins and Blacklisting: Compliance Issues with U.S. Economic Sanction (Part 2),* 5 J. MONEY LAUNDERING CONTROL 66 (2001); P.L. Fitzgerald, *Drug Kingpins and Blacklisting: Compliance Issues with U.S. Economic Sanction (Part 3)*, 5 J. MONEY LAUNDERING CONTROL 162 (2001).

31. Judicial Review Commission on Foreign Asset Control, FINAL REPORT TO CONGRESS, *supra* note 3, at 125-48.

32. *See* Case T-306/01, Yusuf and Al Barakaat International Foundation v. Council and Comm'n, 2005 E.C.R. II-03649.

33. *See* U.S. Treasury Dept., Office of Foreign Assets Control, *Changes to List of*

vigorously questioned the blacklisting through diplomatic channels, arguing that without knowing the actual basis for the U.S. blacklisting decision that triggered these controls, the Swedish government and courts had no way of determining if their nationals were in fact guilty of terrorist involvements, and therefore had no real way of appealing their inclusion on the list.[34]

Although the diplomatic issue was ameliorated by the U.S. asking for the removal of two of the Swedes from the U.N. blacklist in August of 2002, Ahmen Ali Yusuf remained on the list.[35] He sued in the European Court of First Instance alleging numerous procedural flaws and a denial of various guarantees under the European Convention on Human Rights. The Swedish Institute of International Law also issued a Report to the Swedish Foreign Office on Legal Safeguards and Targeted Sanctions strongly suggesting that there were due process issues under the ECHR with the sanctions as formulated and administered.[36] However, the European Court of First Instance broadly rejected Yusuf's claims, and similar subsequent challenges by others, essentially holding that while the E.U. was empowered to impose restrictive measures like economic sanctions on individuals, it was also legally obligated to defer to the U.N.'s blacklisting actions. Moreover, it held that any challenges to those U.N. actions should be directed to the Security Council, as they were outside the Court's scope of review.[37] The U.N.'s intergovernmental process for challenging a blacklist decision under the "Guidelines of the [Sanctions] Committees for the Conduct of Its Work" authorize a government to petition for de-listing on behalf of one of its residents or citizens, but do not expressly provide a blacklisted party with the right to know the basis for that action.[38] If an affected party's

---

Specially Designated Nationals and Blocked Persons Since January 1, 2001, *available at* http://www.ustreas.gov/offices/enforcement/ofac/sdn/sdnew01.pdf.

34. Serge Schmemann, *A Nation Challenged: Sanctions and Fallout; Swedes Take Up the Cause of 3 on U.S. Terror List*, N.Y. TIMES, Jan. 26, 2002, at A9.

35. *See* U.S. Treasury Dept., Office of Foreign Assets Control, *Changes to List of Specially Designated Nationals and Blocked Persons Since January 1, 2002*, *available at* http://www.ustreas.gov/offices/enforcement/ofac/sdn/sdnew02.pdf.

36. *See* Iain Cameron, *Report to the Swedish Foreign Office on Legal Safeguards and Targeted Sanctions*, *supra* note 2.

37. *See* Case T-306/01, Yusuf and Al Barakaat International Foundation v. Council and Comm'n, 2005 E.C.R. II-03649 (Sept. 21, 2005); Case T-315/01, Kadi v. Council and Comm'n, 2005 E.C.R. II-03649 (Sept. 21, 2005); Case T-253/021, Ayadi v. Council and Comm'n, 2005 E.C.R. II-03649 (July 12, 2006).

38. *See* Security Council, Security Council Committee Established Pursuant To Resolution 1267 (1999) Concerning Al-Qaida And The Taliban And Associated Individuals And Entities, Guidelines Of The Committee For The Conduct Of Its Work, *available at* http://www.un.org/Docs/sc/committees/1267/1267_guidelines.pdf. The Guidelines were adopted in November, 2002, and subsequently refined in part due to the concerns raised in the Al Barakaat case.

government refuses to espouse their claim to the U.N. Sanctions Committee, the remedy for that refusal, if any is available, must be determined under domestic national law and procedures.[39]

The European Court's opinions also contain language evidencing an approach that, like the U.S. cases, regards asset blocking or freezing as a foreign policy matter rather than a forfeiture proceeding. The Court stated:

> [i]t is clear that the applicants have not been arbitrarily deprived of [their right to property]. In fact, in the first place, the freezing of their funds constitutes an aspect of the sanctions decided by the Security Council against Usama bin Laden, members of the Al-Qaeda network and the Taliban and other associated individuals, groups, undertakings, and entities. In that regard it is appropriate to stress the importance of the fight against international terrorism and the legitimacy of the protection of the United Nations against the actions of terrorist organizations. . . . The measures in question pursue therefore a legitimate objective of fundamental public interest for the international community. In the second place, freezing of funds is a precautionary measure which, unlike confiscation, does not affect the very substance of the right of the persons concerned to property in their financial assets but only the use thereof.[40]

Despite all his efforts, Ahmen Ali Yusuf remained sanctioned in Europe until the U.S. government announced the removal of his name from its list on August 24, 2006, nearly four years after his initial blacklisting.[41]

Thus, even if the practical and procedural hurdles to judicial review are overcome, the deference given by courts in every jurisdiction to the exercise of executive authority in the area or foreign policy, combined with the traditional regard for sanctions as temporary measures is likely to preclude a reexamination of the blacklisting action. As a result, unless the sanctions programs themselves provide for a review mechanism, these programs are effectively devoid of the procedural and substantive due process protections that would be associated with similar actions if

---

39. The Court noted in the Kahdi case:

> the United Kingdom has quite rightly pointed out at the hearing, it is open to the persons involved to bring an action for judicial review based on domestic law, indeed even directly on the contested regulation and the relevant resolutions of the Security Council which it puts into effect, against any wrongful refusal by the competent national authority to submit their cases to the Sanctions Committee for re-examination. . . .

Case T-315/01 (Sept. 21, 2005) at ¶ 293.

40. Case T-306/01 (Sept. 21, 2005) at ¶ 293-99.

41. *See* U.S. Treasury Dept., Office of Foreign Assets Control, SDGT Designation Removal, *available at* http://www.ustreas.gov/offices/enforcement/ofac/actions/20060824.shtml.

they were taken pursuant to civil or criminal law. However, even if sanctions programs must be regarded as something different from similar measures taken pursuant to civil or criminal law that should not mean that the entire panoply of substantive and procedural protections built into those laws should be abandoned. Post-blacklisting administrative review procedures could afford the affected parties the ability to correct mistakes or address changed circumstances—and provide basic due process of law—without seriously affecting the government's control objectives. However, those mechanisms would need to be built into the sanctions programs themselves, rather than created by the courts. Doing so would provide added credibility to the sanctions programs, which also helps enhance compliance.

E. Uncertainty as to How the Sanctions are Applied and Enforced

The obligations imposed by the current sanctions programs cannot be enforced as broadly as they are written. As a consequence, these programs can suffer from selective and erratic enforcement that undermines voluntary compliance.

While large banking institutions typically have the greatest awareness of the obligations imposed by sanctions and make the greatest efforts to comply with the controls, they are also the most likely to be the focus of governmental enforcement efforts. If governments also desire to promote compliance and cooperation by smaller institutions, non-traditional funds transmitters, and others outside the large institutions at the center of the financial community, their sanctions programs must be more commercially practicable. The reduced compliance that results from a perceived lack of commercial reasonableness is only reinforced when governments then fail to devote the resources required to enforce the sanctions as written, or only selectively enforce them for political ends.

The U.S. Treasury Department's Office of Foreign Assets Control, for example, is a relatively small office with limited resources. What resources they do have are often focused—perhaps largely for domestic political reasons—on the Cuban sanctions, rather than on the anti-terrorist programs. In the last five years, OFAC issued more than a score of regulatory amendments, rulings, or interpretations regarding its Cuban sanctions. This contrasts with only five or six announcements dealing with the substance of its anti-terrorist sanctions programs since the 2001 attacks (apart from adjusting specific blacklist entries) and a roughly equal number of modifications to those programs following the 2006 elections which placed Hamas in control of the Palestinian Authority. Moreover, despite initial successes in blocking or freezing significant

funds, ensuring that the regulated community complies with these controls does not appear to be a priority. Since OFAC began posting summaries of civil enforcement actions on its website in April 2003, by far the largest single category, approximately 300 cases, involve the Cuban sanctions. This compares with only one case under the Terrorism Sanctions Regulations, which resulted in a $2,925 penalty.[42]

Employing multiple blacklisting categories which trigger different levels of restrictive measures might be one way of better tailoring both the controls and the regulated community's compliance obligations. For example, the sanctions applied against the primary target of a sanctions program, such as an Osama bin Laden, could be distinguished from controls applied against a party who only incidentally dealt with or supported the real target of the program. However, under the current programs there is no differentiation between these parties and a secondary or tertiary entity is subject to the same blacklisting and the same controls as the primary target, such as Osama bin Laden.

The U.S. Judicial Review Commission recommended addressing this lack of refinement in the blacklisting controls by distinguishing between what it called Tier I designees, the primary targets of the sanctions, and Tier II designees, those who indirectly deal with the targeted parties. It then suggested that different restrictions, compliance obligations, and opportunities for review might be appropriate for these second-tier blacklist designees—with whom the vast majority of compliance issues arise.[43] The burdens on both government regulators and the regulated community would be reduced and the credibility of these programs enhanced if more refined controls were established distinguishing between the primary and secondary targets of the sanctions.

In addition, if governments regard identifying and tracking questionable funds flows and gathering evidence to prosecute the core targets of the sanctions as important objectives, then there needs to be a way to encourage the voluntary disclosure of information from the regulated community without automatically regarding each disclosure as a noncompliance matter to be handled as a civil penalty case or worse. Rather than imposing strict liability on the regulated community, a combination of establishing *de minimis* levels for compliance violations, recognizing the value of after-the-fact batch blacklist screening in appropriate circumstances, and establishing safe-harbors—or at least an

42. *See* P.L. Fitzgerald, *The Cuban-Thistle Crisis: Rethinking U.S. Sanctions,* 82 FOREIGN SERVICE J. 51 (2005).

43. *See* Judicial Review Commission on Foreign Asset Control, FINAL REPORT TO CONGRESS, *supra* note 3, Recommendations 1-3 at 125-37.

intentional standard for imposing liability—would encourage more disclosures and information sharing between regulators and the regulated community. The current system chills this sort of communication exchange, and therefore undermines the government's ability to use the sanctions as a way to help track questionable money flows.

Large multinational institutions at the core of the financial community are faced with especially complex disclosure issues. Sanctions and enforcement policies for these companies need to be tailored to the risks presented and the nature of their operations. Multinational financial institutions, and separate complex large value transfer systems such as the SWIFT network that links different banking institutions via the U.S. Fedwire or the U.K. CHAPS systems for example, conduct credit transfers which involve multiple transactions. There are many steps involved in moving funds from bank to bank before making a debit transfer to a specific customer. Thus, there may be a series of largely automated transfers and messages related to these inter-bank transactions that are devoid of sufficient individual account/customer identification information to screen against the various sanctions blacklists. It may only be at the very last stage, when a bank is being directed to debit/pay a particular party that the transaction may be matched to the blacklist entries. In such a complex multinational system, under the strict liability standard, it is unclear where the institutional involvement becomes so remote from actual improper action that liability for non-compliance ceases. Moreover, this can be a particularly difficult problem for a multinational commercial entity facing a need to comply with sanctions promulgated by multiple governmental authorities around the world.

In December, 2005, for example, without admitting any culpability, the Dutch bank ABN AMRO N.V. entered into a consent settlement with U.S. authorities for an $80 million civil penalty for alleged violations of the U.S. sanctions on dealings with Iran and Libya.[44] ABN's branches in New York and Chicago cleared payments based upon instructions and documents that originated in ABN's branches in Dubai and India. The Indian and Dubai ABN branches had altered the documents specifically to disguise their involvement with sanctioned parties in Iran and Libya, and also to avoid the transactions being caught by ABN's own internal

44. ABN AMRO Bank N.V. is headquartered in Amsterdam, the Netherlands. The bank has over $500 billion in assets, approximately 111,000 employees and roughly 3,500 offices in over 60 countries. It also maintains several branches, agencies, and offices in the United States. *See* Letter from R.J. Stammer, Vice President and Compliance Officer of ABN AMRO North America to OFAC (July 18, 2002) *available at* http://www.ustreas.gov/offices/enforcement/ofac/interim/civpen/amro.pdf, commenting upon proposed revisions to the publication of civil penalty information.

compliance program. The result was that the overseas Dutch bank paid a significant civil penalty, and incidentally agreed to outside audits and to provide a number of special reports to the U.S. authorities over the next three years, because some employees in its branches in Dubai and India consciously sought to evade ABN's corporate internal compliance program and thus made it impossible for its U.S. branches to maintain strict compliance with the sanctions.[45] Perhaps, most notably, these penalties were all imposed as a result of ABN AMRO's own voluntary disclosure to the U.S. authorities.[46]

The ABN example illustrates some of the difficulties inherent in crafting appropriate internal compliance programs for large enterprises with complex processes, and especially for the network of large value transfer systems, where the full import of the transaction may only become apparent after many innocent steps have been taken. Along with cases such as those involving the Swedish employees of Al Barakaat, it further highlights the need for an official mechanism at the national level that can provide reliable information about the requirements of the various sanctions regimes, and which will help resolve possible conflicts among these laws. As a consequence of the absence of such a mechanism in this case—albeit along with wrongdoing by its local branches in India and Dubai—the Dutch banking enterprise agreed to base the internal compliance programs it creates for its worldwide operations on the obligations imposed by the U.S. controls, even where those controls differ from U.N. or European requirements.

Following the ABN AMRO settlement, other banks, including the London-based HSBC, along with Credit Suisse and UBS in Switzerland, reportedly limited their dealings in Iran in order to avoid issues under U.S. controls, even in the absence of U.N. or European requirements to do so.[47] Other significant fines paid by foreign banks under similar circumstances in the past include the $100 million assessed by U.S. authorities against UBS in 2004 for currency transfers to Cuba, Iran, Libya and the former Yugoslavia, after various employees doctored

45. *See* U.S. Treasury Dept., *Order of Assessment of a Civil Monetary Penalty and Monetary Payment and Order to File Reports Issued Upon Consent involving ABN AMRO Bank N.V,* (Dec. 19, 2005) *available at* http://www.ustreas.gov/offices/enforcement/ofac/civpen/penalties/amrocmp.pdf.

46. *See id.* ABN AMRO did have a pre-existing agreement, dated July 23, 2004, with the Federal Reserve Bank and state authorities in New York and Illinois designed to correct deficiencies at the New York Branch relating to other anti-money laundering policies, procedures, and practices and had taken substantial steps to rectify the deficiencies addressed in that agreement, when it discovered and disclosed the facts relating to the additional transactions that were the subject of this settlement agreement.

47. *See* Steven R. Weisman and Nazila Fathi, *Pressed By U.S., European Banks Limit Iran Deals,* N.Y. TIMES, May 22, 2006, at A1.

records to hide the transactions; and the $200 million fine imposed on the Bank of Credit and Commerce International in 1991 for violating American banking laws on fraud and money laundering.[48]

III. Conclusion

Targeted economic sanctions are powerful tools to augment governmental efforts to address global terrorism and similar intractable international problems. Whether sanctions are regarded as foreign policy measures or as tools addressing international criminality, a number of steps can be taken to enhance their credibility and commercial practicability, and thereby promote more effective and widespread compliance in support of governmental objectives.

These steps include:

1. Formulating sanctions controls on a risk-based model that:
   - distinguishes among the obligations imposed on the various types of businesses or industries comprising the regulated community;
   - distinguishes between the primary targets of the sanctions (e.g. Tier I designees), and secondary or tertiary targets (e.g. Tier II designees); and
   - provides an official mechanism to resolve questionable blacklist matches (on national, international, or foreign blacklists) whose advice may be relied upon by the regulated community.

2. Aligning enforcement practices and resources with those risk-based controls by:
   - establishing governmental standards for liability for non-compliance, or alternatively recognizing industry developed "best practices" for compliance;
   - providing a "safe-harbor" where internal compliance programs are in place which meet such standards or practices; and
   - establishing *de minimis* exemptions for trivial violations, and an intentional or "knowing" standard for liability, that seek to achieve realistic levels of compliance.

48. *See* Timothy L. O'Brien, *Lockboxes, Iraqi Loot And a Trail To the Fed,* N.Y. TIMES, June 6, 2004, at § 3.

3. Creating an official mechanism that:
    - corrects blacklisting mistakes, permits challenges to blacklisting decisions based upon changed circumstances, or that mediates or resolves conflicts among national, international, or foreign sanctions regimes; and
    - encourages more communication and cooperation between the government and the regulated community as partners in addressing these new global threats.

Global terrorism will not be stopped solely by military action or the use of force. Targeted economic sanctions specifically aimed at those who conduct or enable terrorist acts are an integral part of the effort. These sanctions, however, must be designed to have a practical and substantial impact in the marketplace. They cannot simply be broad policy statements focused more on domestic politics than on achieving their stated aims. Doing so means that government regulators and the regulated community must become partners in the effort to a much greater degree than has been the case in the past.