When Comprehensive Falls Short: The Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010

Jennifer M. Kline*

Introduction

In mid-1995, Lloyds TSB Bank, plc ("Lloyds") started manually removing and manipulating the names and addresses of its long-term Iranian banking clients to enable the processing of financial transactions in the United States.[1] Lloyds' "Payment Services Aide Memoire" removes any mention of Iran in wire transfer payments to circumvent the additional time, cost, and difficulty of retrieving assets seized by the United States under the International Emergency Economic Powers Act ("IEEPA").[2] Senior management at Lloyds defended this policy because United States sanctions subjected legitimate Iranian bank transactions to delays and uncertainties.[3] Lloyds is not the only foreign financial institution to knowingly evade United States economic sanctions against Iran and promote its commercial interests.[4] Today there is a constant tension between generating financial profits and promoting United States foreign policy goals to halt the funding of terrorism and the proliferation of weapons of mass destruction ("WMD").

The latest addition to the United States' arsenal of sanctions against Iran is the Comprehensive Iran Sanctions Accountability and Divestment Act of 2010 ("CISADA").5 CISADA consists of a set of targeted economic

∗Jennifer Kline would like to thank Paul Ferman, Michael Hedrick, Aaron Kane, Chrissy Kendall, Stacey Sklaver, and Tyler Stubbs for their help, support, and encouragement on this Comment.

1 Lloyds TSB Bank, plc, Office of Foreign Assets Control, MUL-4745344 (Settlement Agreement) at 2-3 (Dec. 22, 2009), *available at* http://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Documents/lloyds_agreement.pdf.

2 *Id.*

3 *Id.*

4 *See infra* Part II.

5 *See* Comprehensive Iran Sanctions, Accountability, and Divestment Act, 22 U.S.C.A. §§ 8512-31 (West 2010).

sanctions called "smart sanctions."[6] CISADA prohibits or imposes strict conditions on correspondent banking with foreign financial institutions linked to funding Iran's WMD program.[7]

Correspondent banking consists of providing of financial transactions, including deposits and payments, by a United States financial institution for a foreign financial institution[8] that does not have a physical presence in the United States.[9] Correspondent banking runs a high risk of money laundering for illegal activities, including funding Iran's WMD program, because foreign financial institutions can access the United States banking system for a simple fee.[10] Common correspondent banking activities such as wire transfers and payable through accounts ("PTA") are difficult to track.[11] Wire transfers process transactions quickly without screening for the client's identity or the purpose of the transaction, while PTAs allow unidentified subaccount holders in foreign financial institutions to write checks and make deposits in the United States without transactional oversight.[12]

---

6 *See* Peter L. Fitzgerald, *Managing "Smart Sanctions" Against Terrorism Wisely*, 36 NEW ENG. L. REV. 957, 960-61 (2002). Traditional sanctions historically placed trade restrictions on entire countries. Smart sanctions, on the other hand, precisely target key individuals and companies to achieve policy goals in a specific geographic area of concern. This reduces the humanitarian costs often associated with blanket country-wide sanctions. *Id.*

7 H.R. COMM. ON FOREIGN AFFAIRS, 111TH CONG., SUMMARY OF H.R. 2194, THE COMPREHENSIVE IRAN SANCTIONS, ACCOUNTABILITY, AND DIVESTMENT ACT OF 2010, (2010), *available at* http://www.hcfa.house.gov/111/press_062410a.pdf.

8 Iranian Financial Sanctions Regulations, 75 Fed. Reg. 49,836, 49,840 (Aug. 16, 2010) (to be codified at 31 C.F.R. pt. 561).

9 MINORITY STAFF OF THE S. PERMANENT SUBCOMM. ON INVESTIGATIONS, 107TH CONG., REPORT ON CORRESPONDENT BANKING: A GATEWAY FOR MONEY LAUNDERING, at 11 (2001), *available at* http://hsgac.senate.gov/psi_finalreport.pdf.

10 *See* OFFICE OF THE COMPTROLLER OF THE CURRENCY, COMPTROLLER'S HANDBOOK: BANK SECRECY ACT/ANTI-MONEY LAUNDERING, at 21-26 (Dec. 2000), *available at* http://www.occ.gov/static/news-issuances/memos-advisory-letters/2001/pub-advisory-letter-2001-7b.pdf (reporting that correspondent banking with foreign financial institutions runs a high risk of money laundering).

11 *Id.*

12 *Id.*

Transactions shrouded in secrecy are conducive to money laundering. As a result, a comprehensive regulatory system is necessary to combat the risk of money laundering.[13] CISADA limits the ability of foreign financial institutions to assist Iran's WMD program through correspondent banking in the United States,[14] cutting Iran off from important access to the United States financial system. Access to this system is critical for Iran due to the high demand for United States dollars[15] to finance both legitimate and illegitimate[16] Iranian business.[17] If the United States is to achieve its security objectives with respect to Iran's funding of WMD programs, the United States must preclude Iran from using the United States Financial System.

Nonetheless, the effectiveness of CISADA depends on its compliance and enforcement tools. These include auditing, self-reporting, certification,[18] and due diligence.[19] It remains unclear whether these tools

13 *Id.* at 22.

14 Iranian Financial Sanctions Regulations, 75 Fed. Reg. 49,836, 49,837-40 (Aug. 16, 2010) (to be codified at 31 C.F.R. pt. 561).

15 *See* Press Release, U.S. Dep't of the Treasury, Remarks by Treasury Secretary Paulson on Targeted Financial Measures to Protect Our National Security (June 14, 2007), https://ustreas.gov/press/releases/hp457.htm (affirming that the United States is the hub of the global financial system upon which illicit actors rely); *see also* MINORITY STAFF OF THE S. PERMANENT SUBCOMM. ON INVESTIGATIONS, 107TH CONG., REPORT ON CORRESPONDENT BANKING: A GATEWAY FOR MONEY LAUNDERING, at 11-12 (2001), *available at* http://hsgac.senate.gov/psi_finalreport.pdf (stating that most foreign financial institutions use United States dollars and United States correspondent banking accounts to provide international services).

16 *See* S.C. Res. 1929, at 1-4, U.N. Doc. S/RES/1929 (June 9, 2010) (resolving that Iranian efforts to develop a nuclear program are illegitimate because they are violations of international law). In particular, Iran has failed to meet the International Atomic Energy Agency's requirements for information exchange under its safeguard agreement. Iran has further neglected to comply with five United Nations Security Council Resolutions to suspend uranium enrichment activities. *Id.*

17 *See* U.S. Dep't of the Treasury, *supra* note 15 (revealing that financing of Iranian business has fallen dramatically and the risk of financing Iranian business with non-United States currencies remains high).

18 Certification requires United States financial institutions to verify that foreign financial institutions do not engage in prohibited activities.

19 Comprehensive Iran Sanctions, Accountability, and Divestment Act, 22 U.S.C.A. § 8513(e)(1)(A)-(D) (West 2010).

will successfully generate compliance with CISADA and achieve United States national security goals, namely to prevent proliferators accessing the United States financial system to pay for WMD components.[20] CISADA's main enforcement agency, the United States Department of the Treasury's ("Treasury") Office of Foreign Assets Control ("OFAC"),[21] relies on institutional self-reporting of violations as its primary compliance mechanism, making CISADA's effectiveness uncertain.[22]

This comment proposes that self-reporting from the private financial industry creates perverse incentives that CISADA's current compliance tools cannot overcome, largely due to a lack of regulatory clarity and oversight from OFAC. Creation of new legal enforcement tools and clarification of CISADA compliance conditions are necessary to deny Iranian WMD proliferator access to United States correspondent banking accounts.

Part I of this comment provides relevant background information on the applicable money laundering statutes upon which CISADA is modeled. Part II discusses recent bank settlement cases related to violations of United States financial sanctions against Iran. Part III analyzes the lack of incentive for self-reporting and the lack of regulatory clarity and oversight that will impair CISADA's effectiveness in preventing illicit actors from accessing the United States financial system. Finally, part IV proposes legal tools and language clarification to improve compliance with and enforcement of CISADA.

Part I: Background

CISADA's statutory language for restrictions on correspondent banking with foreign financial institutions is modeled closely on existing United States anti-money laundering laws. In particular, CISADA utilizes

20 *See* U.S. DEP'T OF THE TREASURY, STRATEGIC PLAN FISCAL YEARS 2007-2012, at 10, 25, *available at* https://ustreas.gov/offices/management/budget/strategic-plan/2007-2012/strategic-plan2007-2012.pdf (naming the prevention of WMD proliferator access to the United States financial system as a primary national security goal).

21 Iranian Transactions Regulations, 75 Fed. Reg. 59,611, 59,611-12 (Sept. 28, 2010) (to be codified at 31 C.F.R. pt. 360).

22 *See* 22 U.S.C.A. § 8513 (e)(1)(A)(D) (requiring reporting of transactions or suspicious activity under due diligence procedures relating to Iranian proliferation); Fitzgerald, *supra* note 6, at 962-64 (arguing that the effectiveness of OFAC's sanction implementation relies on voluntary compliance, but OFAC and the business community have combative relations).

many of the financial sanctions in Section 311 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act"), which is recognized as the most effective United States legislation for financial "smart sanctions."[23] In turn, much of the USA PATRIOT Act's success is derived from the expansion and amendment of the money laundering principles established by the Bank Secrecy Act of 1970 ("BSA").[24] As a result, it is essential to overview the BSA and USA PATRIOT Act anti-money laundering provisions to understand the implications of CISADA's correspondent banking restrictions more completely.

The BSA was the first federal legislation targeting money laundering.[25] In 1970,[26] Congress enacted the BSA to prevent the use of financial institutions as intermediaries for money laundering and other crimes.[27] The BSA requires financial institutions to keep detailed records of transfers.[28] This paper trail assists United States law enforcement to detect

23 *See* 22 U.S.C.A. § 8513; *see also* USA PATRIOT Act, 31 U.S.C. § 5318(i) (2006) (detailing the due diligence requirements of the USA PATRIOT Act for correspondent banking); COMMITTEE OF CONFERENCE, H.R. COMM. ON FOREIGN AFFAIRS, 111TH CONG., JOINT EXPLANATORY STATEMENT: H.R. 2194, THE COMPREHENSIVE IRAN SANCTIONS, ACCOUNTABILITY, AND DIVESTMENT ACT OF 2010 REPORT, at 18 (2010), *available at* http://www.hcfa.house.gov/111/press_062410d.pdf (describing CISADA's financial institution sanctions as being patterned after the effective section 311 of the USA PATRIOT Act).

24 *See* Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1114 (1970) (codified as amended at 12 U.S.C. §§ 1829b, 1951-59 (2006) and at 31 U.S.C. §§ 5311-32 (2006)); USA PATRIOT Act, Pub. L. No. 107-56, §§ 301-77, 115 Stat. 272, 296-342 (2001) (codified as amended in scattered sections of U.S.C.); *see also* Financial Crimes Enforcement Network, Bank Secrecy Act, http://www.fincen.gov/statutes_regs/bsa (last visited Jan. 11, 2011) (listing the codified amendments to the BSA).

25 *See* Financial Crimes Enforcement Network, History of Anti-Money Laundering Laws, http://www.fincen.gov/news_room/aml_history.html (last visited Jan. 9, 2011).

26 *Id.*

27 OFFICE OF THE COMPTROLLER OF THE CURRENCY, *supra* note 10, at 1. The BSA was enacted to prevent the use of banks as intermediaries for criminal activity such as money laundering and drug trafficking. The modern BSA codifications combats gunrunning, fraud, and terrorism. *Id.*

28 *See* §§ 121, 123, 84 Stat. at 1116-17 (codified as amended at 12 U.S.C. §§ 1951, 1953 (2006)); *see also* OFFICE OF THE COMPTROLLER OF THE CURRENCY, *supra* note 10, at 8-9 (detailing that the BSA requires diligent recordkeeping to reconstruct transactions).

and prevent money laundering and deters United States financial institutions from engaging in illegal activities.[29] Since a financial institution's assets may be subject to forfeiture if traceable to money laundering activities,[30] the BSA's provisions encourage financial institutions to obtain information about potential clients in advance to avoid facilitating money laundering.[31] In addition, the BSA requires financial institutions to make timely reports of suspicious activity related to transactions that might signify money laundering or other illegal activities.[32] Finally, the BSA requires financial institutions to create internal programs for personnel training, independent testing, and internal controls to ensure compliance with the BSA's reporting and recordkeeping requirements.[33] CISADA implements similar recordkeeping and reporting requirements, as well as similar civil and criminal penalty structures for violations.[34]

Congress has amended the BSA several times to enhance its effectiveness,[35] including the expansive anti-money laundering regulations

29 *See* §§ 121, 123, 84 Stat. at 1116-17 (codified as amended at 12 U.S.C. §§ 1951, 1953 (2006)) (recognizing the usefulness of recordkeeping for investigations, proceedings, and intelligence and counterintelligence activities); *see also* OFFICE OF THE COMPTROLLER OF THE CURRENCY, *supra* note 10, at 1 (outlining the use of reporting and recordkeeping to investigate and deter money laundering and illicit activities).

30 *See* §§ 125-27, 84 Stat. at 1117-18 (codified as amended at 12 U.S.C. §§ 1955-57 (2006)); *see also* OFFICE OF THE COMPTROLLER OF THE CURRENCY, *supra* note 10, at 3-4 (reporting that penalties for money laundering include forfeiture).

31 *See* Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1114 (1970) (codified as amended at 12 U.S.C. §§ 1829b, 1951-59 (2006) and at 31 U.S.C. §§ 5311-32 (2006)); *see also* OFFICE OF THE COMPTROLLER OF THE CURRENCY, *supra* note 10, at 1 (declaring that financial institutions must know their clients and their clients' businesses to avoid suspicious activity).

32 Suspicious Activity Report, 12 C.F.R. § 21.11 (2010); Reports by Banks of Suspicious Transactions, 31 C.F.R. § 103.18 (2010); *see also* OFFICE OF THE COMPTROLLER OF THE CURRENCY, *supra* note 10, at 11-12 (noting that the BSA requires diligent reporting of suspicious activity).

33 Procedures for Monitoring Bank Secrecy Act (BSA), 12 C.F.R. § 21.21 (2010); *see also* OFFICE OF THE COMPTROLLER OF THE CURRENCY, *supra* note 10, at 5-7 (stating that internal compliance programs are required to ensure compliance with the BSA).

34 *See* Comprehensive Iran Sanctions, Accountability, and Divestment Act, 22 U.S.C.A. § 8513(e) (West 2010); §§ 121-29, 84 Stat. at 1116-18 (codified as amended at 12 U.S.C. §§ 1951-59 (2006)).

35 OFFICE OF THE COMPTROLLER OF THE CURRENCY, *supra* note 10, at 1.

enacted in 2001 under Title III, the "International Money Laundering Abatement and Anti-Terrorist Financing Act," of the USA PATRIOT Act.[36] Title III contains additional provisions to increase information gathering, recordkeeping, monitoring, reporting, and penalties to counter illegal activities such as money laundering.[37] Subtitle A implements the following international anti-money laundering measures: (1) minimum and enhanced due diligence standards for correspondent accounts; (2) customer identification verification methods; (3) a prohibition on correspondent banking with shell banks;[38] (4) forfeiture of assets and additional penalties for violations of the Act; and (5) improved international cooperation and information sharing for financial institutions.[39] CISADA has expressly incorporated the enhanced due diligence requirements outlined in Subtitle A.[40]

Subtitle B establishes additional amendments and improvements to the BSA,[41] focusing on reporting, anti-money laundering compliance programs, and civil and criminal penalties for violations.[42] Subtitle B

36 *See* USA PATRIOT Act, Pub. L. No. 107-56, §§ 301-77, 115 Stat. 272, 296-342 (2001) (codified as amended in scattered sections of U.S.C.); *see also* Financial Crimes Enforcement Network, USA PATRIOT Act, http://www.fincen.gov/statutes_regs/patriot/index.html (last visited Jan. 10, 2011) (providing an overview of the USA PATRIOT Act provisions impacting financial institutions, including money laundering prevention and prosecution).

37 §§ 301-77, 115 Stat. at 296-342 (codified as amended in scattered sections of U.S.C.).

38 *See* MINORITY STAFF OF THE S. PERMANENT SUBCOMM. ON INVESTIGATIONS, 107TH CONG., REPORT ON CORRESPONDENT BANKING: A GATEWAY FOR MONEY LAUNDERING, at 1, 13 (2001), *available at* http://hsgac.senate.gov/psi_finalreport.pdf (defining a shell bank as a bank with no physical presence, such as an office or staff, in any country). Shell bank transactions are conducted almost entirely through correspondent banking accounts. *Id.* at 13.

39 §§ 311-30, 115 Stat. at 298-320 (codified as amended at 18 U.S.C. § 981 (2006) and at 31 U.S.C. §§ 5318-5318A (2006)).

40 Comprehensive Iran Sanctions, Accountability, and Divestment Act, 22 U.S.C.A. § 8513(e) (West 2010); § 312, 115 Stat. at 304-06 (codified as amended at 31 U.S.C. §§ 5318-5318A (2006)).

41 *See* §§ 351-66, 115 Stat. at 320-36 (Subtitle B); Financial Crimes Enforcement Network, *supra* note 36 (reporting that the USA PATRIOT Act expands liability for reporting).

42 §§ 351-66, 115 Stat. at 320-36 (codified as amended at 31 U.S.C. §§ 5312, 5318, 5321-22 (2006)).

provides for more stringent reporting and recordkeeping obligations for a broader range of financial transactions, including filing reports on currency transactions over $10,000 and systematic reporting of suspicious activities.[43] To help law enforcement prevent and prosecute money laundering activities more efficiently,[44] these requirements apply to banks and non-traditional financial institutions, such as money transmitting businesses, commodity traders, brokers, and dealers.[45] Furthermore, Subtitle B increases civil and criminal penalties for reporting and compliance program violations, creating stronger deterrence of illegal activities for traditional and non-traditional financial institutions.[46] CISIDA incorporates subtitle B's penalties, reporting, and recordkeeping requirements.[47]

Finally, Subtitle C enacts measures to combat currency smuggling and counterfeiting crimes.[48] The main implementation tools are forfeiture and prosecution using extraterritorial jurisdiction.[49] The extraterritorial jurisdiction amends the BSA and the Fraud Statute, 18 U.S.C. § 1029, to apply to any person outside of United States jurisdiction that commits or conspires to commit a fraudulent monetary transaction under United States law using a financial institution within United States jurisdiction.[50] This has particularly important implications for the extraterritorial reach of CISADA.

---

43 §§ 351-66, 115 Stat. at 320-36 (codified as amended at 31 U.S.C. §§ 5312, 5318, 5324, 5331 (2006)).

44 Financial Crimes Enforcement Network, *supra* note 36.

45 *See* §§ 356, 359, 115 Stat. at 324-25, 328-29 (codified as amended at 31 U.S.C. §§ 5312, 5318, 5330 (2006)).

46 *See* § 363, 115 Stat. at 322-23 (codified as amended at 31 U.S.C. §§ 5321-22 (2006)).

47 *See* Comprehensive Iran Sanctions, Accountability, and Divestment Act, 22 U.S.C.A. § 8513(e) (West 2010); §§ 351-66, 115 Stat. at 320-36 (codified as amended at 31 U.S.C. §§ 5312, 5318, 5321-22, 5324, 5330-31 (2006)).

48 §§ 371-77, 115 Stat. at 336-42 (codified as amended at 18 U.S.C. §§ 470-74, 476-82, 484, 493 (2006) and at 31 U.S.C. § 5322 (2006)).

49 §§ 371-72, 377, 115 Stat. at 336-39, 342 (codified as amended at 18 U.S.C. § 1029 (2006) and at 31 U.S.C. §§ 5317, 5322 (2006)).

50 *See* Fraud Statute, 18 U.S.C. § 1029 (2006); Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1114 (1970) (codified as amended at 12 U.S.C. §§ 1829b, 1951-1959 (2006) and at 31 U.S.C. §§ 5311-5330 (2006)); § 377, 115 Stat. at 342 (codified as amended at 18 U.S.C. § 1029 (2006)).

OFAC can now prosecute foreign financial institutions using United States correspondent accounts on behalf of actors linked to Iran's WMD program, regardless of how tangential the relationship may be between the foreign institution and the nefarious actors.[51]

In addition to the above financial regulations under Title III, the USA PATRIOT Act amends IEEPA to enhance OFAC's ability to implement sanctions passed under IEEPA's authority.[52] IEEPA provides the President of the United States with the authority to investigate, regulate, or prohibit financial transfers to a foreign country or national upon declaration of a national emergency stemming from an extraordinary threat to national security, foreign policy, or the economy.[53] The USA PATRIOT Act expands the role of OFAC in executing the President's national emergency powers by clarifying OFAC's authority to block assets of suspicious actors, thus preventing the flight of assets.[54] The USA PATRIOT Act further authorizes OFAC to use classified information to make designations of suspicious actors[55] and to enforce economic and trade sanctions.[56]

CISADA enhances the compliance measures and penalties implemented under the USA PATRIOT Act by extending United States restrictions on foreign financial institution transactions within the United

51 *Cf.* Edward L. Rubinoff and Shiva Aminian, *Recent U.S. and Multilateral Sanctions Against Iran: A New Framework?*, 931 PRACTISING L. INST. 209, 220-21 (2010) (contending that OFAC's extraterritorial reach under CISADA is an extension of the Iranian Transactions Regulations that enable the United States to sanction non-United States persons who have a tenuous connection to the United States).

52 *Counterterror Initiatives in the Terror Finance Program, Focusing on the Role of the Anti-Money Laundering Regulatory Regime in the Financial War on Terrorism, Better Utilization of Technology, Increased Information Sharing, Developing Similar International Standards, and the Formation of Terrorist Financing Operations Section (TFOS) Before the S. Comm. on Banking, Housing & Urban Affairs*, 108th Cong. 193 (2004) (statement of R. Richard Newcomb, Director, Office of Foreign Assets Control).

53 International Emergency Economic Powers Act, 50 U.S.C. §§ 1701-02 (2006).

54 Newcomb, *supra* note 52.

55 *Id.*

56 Office of Foreign Assets Control, About, http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx (last visited on Jan. 11, 2011).

States banking system.[57] CISADA was implemented in part as a response to the Financial Action Task Force's ("FATF") mandate to address new and emerging threats to global financing.[58] FATF imposes strict restrictions on all United States correspondent accounts with foreign financial institutions to prevent money laundering that might facilitate Iranian proliferation efforts.[59] In particular, the statute requires United States financial institutions engaged in correspondent banking with foreign financial institutions to perform audits and report suspicious activities related to Iranian proliferation efforts.[60] Additionally, United States financial institutions must certify that foreign clients are not knowingly engaging in proliferation-related activities and must establish due diligence policies pursuant to the USA PATRIOT Act.[61] Finally, CISADA allows the Secretary of the Treasury to waive restrictions and penalties imposed on foreign financial institutions as necessary for the national interest of the United States.[62]

Ultimately, CISADA is designed to drastically reduce access to the United States financial system by actors intending to finance Iran's WMD program.[63] CISADA is the cumulative effort by the United States

57 *See* Comprehensive Iran Sanctions, Accountability, and Divestment Act, 22 U.S.C.A. §§ 8513 (West 2010); *see also* COMMITTEE OF CONFERENCE, H.R. COMM. ON FOREIGN AFFAIRS, 111TH CONG., JOINT EXPLANATORY STATEMENT: H.R. 2194, THE COMPREHENSIVE IRAN SANCTIONS, ACCOUNTABILITY, AND DIVESTMENT ACT OF 2010 REPORT, at 18-19 (2010), *available at* http://www.hcfa.house.gov/111/press_062410d.pdf (describing CISADA's financial institution sanctions as offensively extending the USA PATRIOT Act measures to foreign financial institutions).

58 *See* 22 U.S.C.A. § 8513. The intergovernmental organization FATF develops policies to combat evolving financial system threats, such as money laundering and terrorist and WMD proliferation financing. In February 2010, the FATF appealed to its members to protect their correspondent accounts, which might be used by Iran to circumvent money laundering and terrorism countermeasures. *Id.*

59 22 U.S.C.A. § 8513.

60 *Id.*; *see* USA PATRIOT Act, 31 U.S.C. § 5318(i)(2)(B)(ii) (2006) (requiring United States financial institutions to report suspicious transactions).

61 22 U.S.C.A. § 8513; *see* 31 U.S.C. § 5318(i).

62 22 U.S.C.A. § 8513.

63 H.R. COMM. ON FOREIGN AFFAIRS, 111TH CONG., SUMMARY OF H.R. 2194, THE COMPREHENSIVE IRAN SANCTIONS, ACCOUNTABILITY, AND DIVESTMENT ACT OF 2010, (2010), *available at* http://www.hcfa.house.gov/111/press_062410a.pdf; U.S. DEP'T OF THE TREASURY, *supra* note 20.

government to counteract money laundering and illicit financial transactions that undermine national security.[64] As a result, the statute targets correspondent banking transactions using tools enacted by the BSA and the USA Patriot Act: reporting and due diligence requirements; civil and criminal penalties; and extraterritorial jurisdiction.[65]

Part II: Case Studies of United States Sanction Enforcements Against Foreign Banks

Before examining CISADA's specific implementation issues, it is useful to understand the trend in recent OFAC financial sanction enforcement cases. Since December 2009, OFAC has announced three settlements concerning major international banks that violated IEEPA regulations related to Iran.[66] Brief case studies of OFAC's settlements with Credit Suisse AG ("Credit Suisse"), Lloyds, and Barclays Bank PLC ("Barclays") reveal that self-reporting of financial sanction violations remains sporadic.[67] Furthermore, foreign financial institutions intentionally remove or manipulate client identification information to evade financial sanctions.[68]

The first OFAC settlement case in this series of financial sanction enforcements against Iran involved the Swiss bank, Credit Suisse.[69] Credit Suisse contacted OFAC in 2006 concerning a potential sanction violation

64 *See* 22 U.S.C.A. §§ 8512-31 (West 2010); *supra* notes 20, 25, 36 and accompanying text.

65 *See* 22 U.S.C.A. §§ 8512-31; Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1114 (1970) (codified as amended at 12 U.S.C. §§ 1829b, 1951-59 (2006) and at 31 U.S.C. §§ 5311-32 (2006)); USA PATRIOT Act, Pub. L. No. 107-56, §§ 301-77, 115 Stat. 272, 296-342 (2001) (codified as amended in scattered sections of U.S.C.).

66 Barclays Bank PLC, Office of Foreign Assets Control, MUL-488066 (Settlement Agreement), at 1-7 (Aug. 18, 2010) *available at* https://ustreas.gov/offices/enforcement/ofac/civpen/penalties/08182010.pdf; Lloyds TSB Bank, plc, *supra* note 1, at 1-8; Credit Suisse AG, Office of Foreign Assets Control, MUL-473923 (Settlement Agreement), at 1-9 (Dec. 16, 2009), *available at* https://ustreas.gov/offices/enforcement/ofac/civpen/penalties/12162009.pdf.

67 Barclays Bank PLC, *supra* note 66; Lloyds TSB Bank, plc, *supra* note 1, at 1-8; Credit Suisse AG, *supra* note 66.

68 *Id*.

69 Credit Suisse AG, *supra* note 66.

involving United States securities.[70] In its investigation, OFAC discovered that Credit Suisse had also systematically violated United States fund transfer restrictions with Iran since the 1990s.[71] Specifically, Credit Suisse omitted or removed location and entity information from fund transfer forms to conceal the identity of an Iranian bank as the originator of the fund transfer requests. Credit Suisse then referenced itself as the ordering institution instead.[72] Credit Suisse even developed an internal operating procedure specifically to evade United States sanctions.[73] This system utilized code names and limited the personnel who knew the Iranian client's identification, deliberately excluding Credit Suisse's compliance department from this knowledge.[74] In order to avoid criminal prosecutions for these calculated sanction violations, Credit Suisse agreed to pay a $536 million fine, create an electronic database of internal documents related to the fund transfers from 2002 to 2007, and implement and certify sanction compliance training and a written bank-to-bank payment transfer policy.[75]

Less than a week later, OFAC announced another settlement for Iranian financial sanction violations by the United Kingdom's Lloyds bank.[76] Lloyds manipulated and deleted wire transfer information relating to Iranian bank clients from the early 1980s until November 2003.[77] Lloyds' senior management continued to remove information to expedite wire transfers and intentionally evade OFAC filters designed to detect identification information for sanctioned actors.[78] The New York County District Attorney's Office apprised OFAC of these IEEPA violations in

70 *Id.* at ¶ 3.

71 *Id.* at ¶¶ 3, 4, 7.

72 *Id.* at ¶ 8.

73 *Id.* at ¶ 13.

74 *Id.*

75 Credit Suisse AG, Office of Foreign Assets Control, MUL-473923, (Deferred Prosecution) ¶¶ 3, 6 (Dec. 16, 2009), *available at* http://www.jdsupra.com (search for "MUL-473923").

76 Lloyds TSB Bank, plc, *supra* note 1.

77 *Id.* at ¶¶ 6, 12, 13.

78 *Id.* at ¶ 8.

2007 and OFAC investigated.[79] Lloyds ultimately agreed to pay a $217 million settlement, provide all United States payment messages from 2002 to 2007 to OFAC, and implement an annual audit of United States payments with an independent consultant.[80]

Finally, OFAC settled with the United Kingdom's Barclays in August 2010 for violations of IEEPA financial sanctions relating to Iran.81 Barclays voluntarily disclosed its sanction violations to OFAC in May 2006.[82] The voluntary disclosure revealed that Barclays systematically obscured and removed identification information of sanctioned Iranian financial institutions, including Iran's Central Bank, from 1987 until at least 2004.[83] Barclays also utilized a wire transfer filter to identify and interdict sanctioned party transactions in order to remove offending information or substitute Barclay's sundry account number prior to processing payments.[84] Barclays agreed to pay a $176 million fine and annually review its policy and procedures for sanctions compliance with an independent consultant.[85] The settlement also included employee training to deal with United States financial sanctions and the creation of a database of United States payment messages from 2000 to 2007.[86]

As illustrated, foreign financial institutions are intentionally and systematically evading Iranian financial sanctions.[87] These case studies further demonstrate how OFAC's enforcement of financial sanctions relies heavily upon voluntary disclosures or information provided by other

79 *Id.* at ¶ 3.

80 *Id.* at ¶¶ 5, 17-19.

81 Barclays Bank PLC, *supra* note 66.

82 *Id.* at ¶ 3.

83 *Id.* at ¶¶ 4-6.

84 *Id.* at ¶¶ 7, 8.

85 *Id.* at ¶¶ 21, 22.

86 Barclays Bank PLC, Office of Foreign Assets Control, MUL-488066, (Deferred Prosecution) ¶ 7 (Aug. 18, 2010), *available at* http://www.courthousenews.com /2010/08/19/Barclays.pdf.

87 Barclays Bank PLC, *supra* note 66; Lloyds TSB Bank, plc, *supra* note 1, at 1-8; Credit Suisse AG, *supra* note 66.

government agencies.[88] Although Barclays voluntarily disclosed its intentional removal and manipulation of identification information to circumvent United States sanctions,[89] Credit Suisse's institutionalized efforts to evade Iranian financial sanctions were only discovered as part of an investigation of a different violation.[90] This relatively haphazard approach to sanction enforcement is indicative of the potential implementation issues OFAC will face in trying to implement CISADA effectively for correspondent banking functions.

Fortunately, the studies also reveal that OFAC's enforcement of financial sanctions resulted in high settlement payments, as well as provisions for continued oversight by OFAC for the violating institutions.[91] Credit Suisse, in particular, agreed to a hefty $536 million fine,[92] which may deter correspondent banking violations under CISADA in the first place. In addition, since Barclays paid less than a quarter of Credit Suisse's settlement fine for virtually identical sanction violations[93] other financial institutions currently in violation of CISADA may choose to disclose their violations rather than wait to be detected. Nonetheless, OFAC's reliance on sanction enforcement by other agencies and voluntary compliance by

88 *Id*.

89 Barclays Bank PLC, *supra* note 66, ¶¶ 3-6.

90 Credit Suisse AG, *supra* note 66.

91 *See* Barclays Bank PLC, *supra* note 66; Lloyds TSB Bank, plc, *supra* note 1, at 1-8; Credit Suisse AG, *supra* note 66; Australia and New Zealand Banking Group, Ltd., Office of Foreign Assets Control, MUL-464334 (Settlement Agreement), at 2-3 (Aug. 21, 2009), *available at* http://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Documents/anz_08242009.pdf; ABN AMRO Bank N.V., Financial Crimes Enforcement Network, No. 2005-5 (Assessment of Civil Money Penalty), at 3, 7-8 (Dec. 19, 2005), *available at* http://www.fincen.gov/news_room/ea/files/abn_assessment.pdf; Office of Foreign Assets Control, Civil Penalties Information, https://ustreas.gov/offices/enforcement/ofac/civpen/index.shtml (follow the hyperlinks for OFAC Enforcement Actions By Year) (providing information on OFAC's five financial institution sanction enforcement cases since 2003 that resulted in settlement payments and agreements for OFAC monitoring of compliance programs and independent audits).

92 Credit Suisse AG, *supra* note 75, ¶ 3.

93 Barclays Bank PLC, *supra* note 66; Credit Suisse AG, *supra* note 66.

financial institutions[94] poses serious concerns for the proper implementation and enforcement of CISADA.

Part III: Implementation Issues – the Lack of Institutional Incentive

CISADA, like its statutory predecessors, relies on financial institutions to self-report suspicious activities concerning client transactions in order to meet their reporting, compliance program, and certification obligations.[95] Unfortunately, financial institution incentives to comply with additional monetary transaction restrictions do not inherently coincide with the U.S. foreign policy objectives underlying the promulgation of CISADA. In fact, CISADA's main foreign policy objective of blocking Iranian WMD proliferation access to the United States financial system[96] leaves no room for financial institutions to consider profit margins or entrepreneurialism. Although CISADA provides for stringent civil and criminal penalties,[97] the specter of monetary fines and imprisonment may be insufficient to deter financial institutions from pursuing profitable correspondent banking activities with questionable foreign financial institutions. This would almost certainly undermine self-reporting mechanisms as the primary line of defense against illicit utilization of correspondent bank accounts.

CISADA's threatened penalties may be insufficient for several reasons. First, financial institutions are private institutions that must remain competitive in order to survive. Much like any private corporation, financial institutions undergo a cost-benefit analysis in determining to what extent they will comply with sanctions.[98] As a result, financial institutions must balance tangible and intangible costs and benefits when determining whether to pursue transactions potentially linked to Iranian proliferation.

---

94 Barclays Bank PLC, *supra* note 66; Lloyds TSB Bank, plc, *supra* note 1; Credit Suisse AG, *supra* note 66.

95 *See* Comprehensive Iran Sanctions, Accountability, and Divestment Act, 22 U.S.C.A. § 8513 (West 2010) (referencing USA PATRIOT Act, 31 U.S.C. § 5318(i) (2001)); *supra* notes 32-33, 42-43 and accompanying text.

96 U.S. DEP'T OF THE TREASURY, *supra* note 20.

97 22 U.S.C.A. § 8513(e)(2).

98 *See* Fitzgerald, *supra* note 6, at 981 (arguing that in a competitive marketplace even legitimate businesses will be disinclined to comply with regulations unless their competitors do the same, especially when the risk of being detected for a violation appears low).

Second, the incentives to comply with the statute are not apparent given the ambiguity in CISADA's language and OFAC's relatively weak implementation capabilities.

A. Tangible and Intangible Cost-Benefit Considerations

Cost-benefit analysis for financial institutions focuses in large part on tangible concerns, such as the potential loss of profits due to the exclusion of transactions with certain foreign clients.[99] Due to the severe consequences of illicitly assisting Iranian actors,[100] a high profit margin exists for risky financing of Iranian actors through correspondent banking accounts.[101] In addition, sanctions put United States companies at a competitive disadvantage with respect to potentially lucrative projects in Iran.[102] Indeed, the costs of sanctions can be very large for United States financial institutions, especially when a major economic force, such as Iran and its oil market, is prohibited from United States investment or financial transactions.[103] Based on these incentives, financial institutions are disinclined to perform extensive due diligence that limits their business operations and profitability with foreign financial institutions if they do not think their competitors will do the same.[104]

---

99 *See* Charles Breckinridge, *Sanction First, Ask Questions Later: The Shortsighted Treatment of Iran Under the Iran and Libya Sanctions Act of 1996*, 88 GEO. L.J. 2439, 2460 (2000) (stating that sanctions commercially injure United States companies that cannot participate in valuable Iranian projects).

100 *See* Orde F. Kittrie, *New Sanctions for a New Century: Treasury's Innovative Use of Financial Sanctions*, 30 U. PA. J. INT'L L. 789, 797-98 (2009) (detailing that eighty banks globally have withdrawn from Iran and leading financial institutions have scaled back their business with Iran).

101 *Cf.* Breckinridge, *supra* note 99, at 2460-62 (illustrating how companies that avoided United States sanctions have obtained lucrative Iranian projects).

102 *See id.* (declaring that United States companies were excluded from valuable Iranian projects because of sanctions).

103 *See* CONGRESSIONAL BUDGET OFFICE, THE DOMESTIC COSTS OF SANCTIONS ON FOREIGN COMMERCE, at IX, 6, 10 (1999), *available at* http://www.cbo.gov/ftpdocs/11xx/doc1133/tradesanc.pdf (reporting that sanctions increase the cost of foreign investment and exporting and importing goods and services to sanctioned companies, particularly in markets with no readily available substitutes).

104 *See* Fitzgerald, *supra* note 6, at 981 (contending that in a competitive marketplace businesses will be disinclined to screen all transactions in compliance with regulations unless their competitors do the same).

The lack of available information about OFAC sanction enforcement cases further complicates the cost-benefit analysis of lucrative correspondent banking accounts, leading financial institutions to feel insulated from the risk of being detected for violations.[105] In particular, OFAC does not publicize information about the effectiveness of its sanctions implementation efforts, making the risk of prosecution appear minimal.[106] Until the early 1990s, OFAC only directly provided major commercial banks with information about rules implementing sanctions.[107] OFAC also posted notices of licenses and changes in the Treasury Department Annex Building[108] and responded to inquiries from other institutions that had compliance questions.[109] Even today, OFAC uses a variety of distribution methods that contain varying levels of detail, including the Federal Register, press releases, and OFAC's website.[110]

OFAC also does not enforce economic sanction regulations strictly due to resource constraints and policy considerations of balancing business needs[111] with anti-terrorism and nonproliferation objectives.[112] In the past, the United States' interest in avoiding conflicts with companies and political allies resulted in erratic enforcement of financial sanctions.[113] More importantly, OFAC has a lack of funding for its ever-enlarging role as the implementation and enforcement branch of economic sanctions.[114]

---

105 *See* Fitzgerald, *supra* note 6, at 981 (maintaining that businesses perceive the risk of OFAC enforcement of a sanction violation as low).

106 *Id.*

107 Peter 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 HASTINGS L.J. 73, 120-21 (1999).

108 *Id.* at 121.

109 *Id.*

110 *See id.* at 123, 128.

111 Fitzgerald, *supra* note 6, at 963, 980-81.

112 U.S. DEP'T OF THE TREASURY, *supra* note 20.

113 *See* Breckinridge, *supra* note 99, at 2452 (citing the Clinton administration's sporadic enforcement of the Iran and Libya Sanctions Act to avoid upsetting foreign allies).

114 *See* Fitzgerald, *supra* note 6, at 962 (outlining the funding issues for OFAC's vast sanction program duties that impair OFAC's ability to handle additional sanctions); Office

OFAC's workforce and budget are distributed among licensing and sanction program responsibilities, in addition to enforcing civil penalties for violations.[115] Furthermore, OFAC oversees nineteen sanction programs.[116] As a result of OFAC's limited capacity to oversee and enforce its numerous sanction programs,[117] it is likely that financial institutions are going to trivialize the risk of being prosecuted for a violation of CISADA. It may be quite profitable to pursue risky behavior due to this low likelihood of penalties, and, as a result, the incentive to self-report violations is virtually nonexistent.

Despite an increase in suspicious activity reports filed by financial institutions since the enactment of the USA PATRIOT Act in 2001,[118] due diligence has not necessarily improved.[119] Rather, financial institutions may be participating in "defensive filing" to protect themselves from penalties without improving their oversight.[120] As a result, OFAC must now sift

---

of Foreign Assets Control, *supra* note 56.

115 Office of Foreign Assets Control, Civil Penalties and Enforcement Information, http://www.treasury.gov/resource-center/sanctions/CivPen/Pages/civpen-index2.aspx (last visited on Jan. 13, 2011); Office of Foreign Assets Control, Sanctions Programs, http://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx (last visited on Jan. 13, 2011); *see* Office of Foreign Assets Control, OFAC Reporting and License Application Forms, http://www.treasury.gov/resource-center/sanctions/Pages/forms-index.aspx (last visited on Jan. 13, 2011) (providing license applications relating to sanctioned country programs).

116 Office of Foreign Assets Control, Sanctions Programs, http://www.treasury.gov /resource-center/sanctions/Programs/Pages/Programs.aspx (last visited on Jan. 13, 2011).

117 Fitzgerald, *supra* note 6, at 962.

118 FINANCIAL CRIMES ENFORCEMENT NETWORK, THE SAR ACTIVITY REVIEW: BY THE NUMBERS (2008), *available at* http://www.fincen.gov/news_room/rp/files/sar_by_numb_09.pdf (showing a growth of over five times the number of suspicious activity reporting from 2001 to 2006).

119 *See* Michael Levi & Peter Reuter, *Money Laundering*, 34 CRIME & JUST. 289, 340-42 (2006) (suggesting that the increase in suspicious activity reporting may be a result of banks filing to protect themselves without improving due diligence).

120 *See* Indranil Ganguli et al., *Third AML-Directive: Europe's Response to the Threat of Money Laundering and Terrorist Financing: Part III*, 126 BANKING L.J. 787, 813-14 (2009) (describing the trend in over-compliance with suspicious activity reporting by United States financial institutions to avoid the risk of fines); Levi, *supra* note 119 (noting that an increase in suspicious activity reporting to protect banks may not correlate with improved due diligence efforts).

through an even higher volume of potentially non-credible suspicious activity reports in order to find legitimate threats, further taxing OFAC's capacity.[121]

The cost-benefit analysis of complying with financial regulations on correspondent banking accounts also includes intangible considerations, such as damage to an institution's reputation should it be prosecuted for violating CISADA.[122] The damage to reputation could be devastating given the highly emotional United States foreign policy objectives behind CISADA: the prevention of instability and danger that will almost certainly exist if Iran, a sponsor of extraterritorial terrorism, successfully develops a nuclear weapons program.[123] In addition, foreign financial institution violators could damage the reputation of countries in which they are jurisdictionally domiciled, potentially causing political and financial conflicts for countries that have supported United Nations sanctions against Iran's nuclear program.[124]

Finally, the cost-benefit analysis for financial institutions includes the actual costs of complying with the strict financial sanctions under CISADA.[125] OFAC creates a new set of regulations every time new economic sanctions must be implemented.[126] However, OFAC has not

121 *Cf.* Ganguli, *supra* note 120 (warning that the increased number of tenuously based suspicious activity reports poses a serious challenge to the Financial Crimes Enforcement Network's institutional capacity).

122 *See* Benjamin Mojuye, *What Banks Need to Know About the Patriot Act*, 124 BANKING L.J. 258, 272 (2007) (stating that financial institutions will likely suffer severe reputation damage for anti-money laundering sanction violations).

123 *See* U.S. DEP'T OF THE TREASURY, *supra* note 20 (emphasizing the threat an Iranian nuclear weapon poses to United States and global security); Andrew Hudson, *Not a Great Asset: The UN Security Council's Counter-Terrorism Regime: Violating Human Rights*, 25 BERKELEY J. INT'L L. 203, 206 (2007) (reporting on the stigma attached to being a terrorist supporter); U.S. Department of State, Background Note: Iran, http://www.state.gov/r/pa/ei/bgn/5314.htm (last visited Jan. 13, 2011) (declaring that Iran is known for supporting terrorism abroad).

124 *See* Kittrie, *supra* note 100, at 816-17 (emphasizing the reputational risk to foreign financial institutions and foreign governments of handling illicit business with Iran that is contrary to international law); U.S. Dep't of the Treasury, *supra* note 20.

125 *See* Peter L. Fitzgerald, *Smarter "Smart" Sanctions*, 26 PENN ST. INT'L L. REV. 37, 51 (2007) (arguing that OFAC needs to make the sanction compliance costs for financial institutions more commercially feasible).

126 Fitzgerald, *supra* note 6, at 966.

collaborated with the regulated community to ensure that implementation is commercially practicable for all members.[127] The burden of performing audits, reporting, certification, and due diligence in determining the identification and innocence of all users of a correspondent banking account under CISADA may be prohibitive for smaller financial institutions.[128]

The implementation costs for CISADA are diverse. Compliance program costs include: (1) additional personnel for oversight; (2) personnel training to identify and manage correspondent banking risks; (3) software for automated review of wire transfers; and (4) productive hours spent on performing compliance tasks, including filing forms, certification, coordination between bankers and compliance personnel, and creating effective implementation programs.[129] All of these costs potentially detract from a financial institution's ability to engage in activities that are more profitable. In addition, the virtually limitless amount of public information available about certain foreign financial institutions could make performance of due diligence prohibitively time consuming and expensive.[130] Furthermore, obtaining certification that foreign financial institutions do not provide services to shell banks[131] and obtaining lists of foreign bank customers may be impracticable under foreign bank secrecy laws in certain countries.[132]

---

127 Fitzgerald, *supra* note 6, at 964, 981 (advising OFAC to consult with the regulated community to determine what compliance programs would not be overly burdensome).

128 22 U.S.C.A. § 8513(e)(1)(A-D); *cf.* Robert E. O'Leary, *Improving the Terrorist Finance Sanctions Process*, 42 N.Y.U. J. INT'L L. & POL. 549, 568 (2010) (asserting that the burden on small charities to ensure the final use of its contributions will not violate sanctions may be too high).

129 *See* MINORITY STAFF OF THE S. PERMANENT SUBCOMM. ON INVESTIGATIONS, 107TH CONG., REP. ON CORRESPONDENT BANKING: A GATEWAY FOR MONEY LAUNDERING, at 1, 11, (2001), *available at* http://hsgac.senate.gov/psi_finalreport.pdf.

130 Special Due Diligence Programs for Certain Foreign Accounts, 71 Fed. Reg. 496, 502 (Jan. 4, 2006).

131 Correspondent Accounts for Foreign Shell Banks, 67 Fed. Reg. 60,562, 60,568 (Sept. 26, 2002) (to be codified at 31 C.F.R. pt. 103).

132 *See* Special Due Diligence Programs for Certain Foreign Accounts, 72 Fed. Reg. 44,768, 44,771 (Aug. 9, 2007) (outlining potential issues obtaining lists of foreign bank customers for correspondent banking accounts because of privacy laws in foreign countries); *see also* MINORITY STAFF OF THE S. PERMANENT SUBCOMM. ON

OFAC has responded to these concerns by emphasizing a risk-based approach to the implementation of CISADA regulations.[133] This approach focuses on the history of the foreign financial institution's practices, as well as the nature of the correspondent banking account, to determine the probability that the foreign financial institution will engage in illicit correspondent banking activities.[134] Unfortunately, this highly discretionary risk-based approach highlights a major challenge to successful implementation of CISADA. The lack of clear obligations in the regulatory language of CISADA undermines compliance due to general uncertainty concerning requirements and the possibility of abuse of language ambiguities.[135] This is particularly problematic because the success of the reporting, certification, and compliance program requirements under CISADA[136] depends almost exclusively on self-reporting by financial institutions.[137] Financial institutions are faced with a compliance paradigm that provides an incentive to cheat: either over-comply with suspicious activity reporting to avoid violation penalties without improving due diligence procedures[138] or avoid self-reporting entirely since it is statistically unlikely that OFAC will enforce any violations.[139] As a result,

---

INVESTIGATIONS, 107TH CONG., REP. ON CORRESPONDENT BANKING: A GATEWAY FOR MONEY LAUNDERING, at 39-40, (2001), *available at* http://hsgac.senate.gov/psi_finalreport.pdf (finding that bank secrecy laws stop the flow of information necessary to identify money launderers).

133 *See* Special Due Diligence Programs for Certain Foreign Accounts, 71 Fed. Reg. at 502 (regulating that United Stated financial institutions must maintain adequate due diligence policies and procedures to evaluate the money laundering risks posed by correspondent accounts and to detect and report any suspected or known money laundering activity under OFAC's risk-based approach to implementing CISADA). Factors to consider in the risk-based approach include the nature of: (1) the foreign financial institution's business and markets; (2) the United States institution's relationship with the foreign institution; and (3) the correspondent account type. *Id.*

134 *Id.* at 502-03.

135 *See* Fitzgerald, *supra* note 125, at 38 (positing that greater certainty regarding regulatory obligations would improve compliance).

136 Comprehensive Iran Sanctions, Accountability, and Divestment Act, 22 U.S.C.A. § 8513(e)(1)(B)-(D) (West 2010).

137 *See id.* § 8513(e)(1)(B); Fitzgerald, *supra* note 6, at 964 (stating that the effectiveness of OFAC's regulations depends more upon voluntary compliance by businesses than OFAC enforcement).

138 Ganguli, *supra* note 120.

139 *Cf.* Fitzgerald, *supra* note 6, at 981 (arguing that businesses will not screen all

financial institutions may become complacent in reviewing their correspondent banking accounts,[140] with potentially dire consequences for United States national security.[141]

B. Mixed Incentives Stemming from Ambiguous Language and Requirements

The lack of clarity in CISADA's statutory language and subsequent OFAC regulations creates additional uncertainty for financial institutions beyond the confusion caused by OFAC's ambiguous risk-based approach to implementation.[142] For instance, certification that a foreign financial institution's customer is not knowingly engaging in activity to assist Iran's WMD program is required to be "to the best of the knowledge of the domestic financial institution."[143] This gives little guidance about the minimum requirements that qualify as having "knowledge" about illegal correspondent banking activities under CISADA.[144]

OFAC recently attempted to address this problem by promulgating definitions for terms in CISADA. OFAC designated "knowingly" to mean that an actor had "actual knowledge, or should have known, of the conduct, the circumstance, or the result."[145] Even though "actual knowledge" is

---

transactions in compliance with regulations in order to remain competitive, especially when the risk of OFAC enforcement of a sanction violation is perceived as low).

140 *Cf.* Lawrence A. Cunningham, *Evaluation and Response to Risk by Lawyers and Accountants in the U.S. and E.U.*, 29 J. Corp. L. 267, 305 (2004) (explaining that audit controls under the USA PATRIOT Act provide assurances but also can create complacency).

141 *See* U.S. DEP'T OF THE TREASURY, *supra* note 20 (emphasizing the importance of freezing money intended for WMD proliferation).

142 *See* Special Due Diligence Programs for Certain Foreign Accounts, 72 Fed. Reg. 44,768, 44,769 (Aug. 9, 2007) (highlighting privacy laws in foreign countries that may inhibit identifying all correspondent bank account users through due diligence); Special Due Diligence Programs for Certain Foreign Accounts, 71 Fed. Reg. 496, 502 (Jan. 4, 2006) (elucidating concerns about due diligence procedures); Correspondent Accounts for Foreign Shell Banks, 67 Fed. Reg. 60,562, 60,568 (Sept. 26, 2002) (to be codified at 31 C.F.R. pt. 103) (commenting on potential certification issues).

143 Comprehensive Iran Sanctions, Accountability, and Divestment Act, 22 U.S.C.A. § 8513(e)(1)(C) (West 2010).

144 22 U.S.C.A. § 8513(e)(1)(C).

145 Iranian Financial Sanctions Regulations, 75 Fed. Reg. 49,836, 49,840 (Aug. 16, 2010)

usually interpreted to mean "direct or clear knowledge,"[146] the definition for "should have known" in OFAC's regulations remains discretionary. The term "should have known" could refer to constructive knowledge acquired when "a person exercising due diligence should have discovered the probability" or had "reason to suspect the probability of any manner of wrongdoing."[147] However, the term could instead refer to a person acquiring knowledge through actual perception or observation of the event or activity.[148] These varied standards of knowledge enable financial institutions to determine their compliance with CISADA in a number of different ways, depending on what is most convenient to their purposes, which will likely result in less effective overall implementation of the statute.

CISADA's statutory language is equally ambiguous when defining due diligence requirements, referring simply to the USA PATRIOT Act's due diligence procedures.[149] Under the USA PATRIOT Act, there is a requirement of general due diligence to identify actors and report suspicious activities.[150] The procedures for general due diligence only expressly include the use of "appropriate" policies and procedures to detect money laundering and ascertain the identity of nominal and beneficial owners.[151] The difficulty in interpreting these due diligence standards under CISADA becomes apparent in the implementation stage. The term "appropriate" gives virtually unlimited discretion to financial institutions to determine how actively they will monitor correspondent banking accounts for statutory compliance.

Fortunately, CISADA also incorporates the enhanced due diligence requirements under the USA Patriot Act, which are more clearly written.

(to be codified at 31 C.F.R. pt. 561).

146 Williams v. Great W. Cas. Co., No. 5:08CV137, 2009 WL 4927710, at *4 (N.D.W. Va. 2009).

147 Zola v. Gordon, 685 F. Supp. 354, 367 (S.D.N.Y. 1988).

148 *See* United State v. Sinclair, 109 F. 3d 1527, 1536 (10th Cir. 1997).

149 22 U.S.C.A. § 8513(e)(1)(D) (referencing USA PATRIOT Act, 31 U.S.C. § 5318(i) (2006)).

150 31 U.S.C. § 5318(i)(3)(A)-(B).

151 *Id.* § 5318(i)(1)(3)(A).

Enhanced due diligence applies if the actor has been specifically designated by OFAC as requiring special measures relating to money laundering concerns. Enhanced due diligence is also required if the actor has an offshore banking license that prohibits conducting banking activities on-shore with the country that issued the license.[152] The enhanced due diligence procedures are more specific than the general due diligence procedures, and it limits application to pre-designated and offshore actors. These procedures require United States financial institutions to determine the identity of all owners of the foreign bank and any additional foreign financial institutions using that bank for correspondent banking activities.[153] United States financial institutions must also conduct enhanced scrutiny of account activities under these due diligence procedures.[154]

Importantly, while the enhanced due diligence procedures are relatively straightforward, the majority of due diligence implementation will occur under the regular due diligence requirements. If an actor is not blacklisted by OFAC or operating on an offshore license, the actor is not subject to enhanced due diligence requirements. Financial institutions must determine what constitutes "appropriate" due diligence procedures and to whom those procedures should apply. This makes implementation of CISADA due diligence requirements discretionary and likely inconsistent among financial institutions.

Overall, the perceived costs and benefits of compliance with CISADA for financial institutions make effective implementation and self-reporting of violations unlikely. Difficulties in interpreting how to implement CISADA, lack of OFAC enforcement and oversight, costs of compliance programs, and potential loss of profits weigh heavily against effective implementation and compliance. Greater oversight and enforcement that is more stringent are needed to increase reputational costs and tip the cost-benefit analysis for financial institutions towards full compliance.

152 *Id.* § 5318(i)(2)(A)(i)-(ii).

153 *Id.* § 5318(i)(2)(B)(i)(iii).

154 *Id.* § 5318(i)(2)(B)(ii).

Part IV: Measures to Enhance CISADA Effectiveness Domestically

Implementation of three key enforcement tools and legal standards could enhance CISADA's effectiveness: (1) an enforcement body in OFAC; (2) a safe harbor clause for innocent mistakes resulting in violations of CISADA; and (3) clarified statutory language.

A. Enforcement Body

OFAC needs an enforcement body to gather intelligence and investigate suspected violations.[155] Currently, OFAC relies upon information from self-reporting financial institutions[156] and coordination with other government agencies, including the Departments of State, Defense, Commerce, Homeland Security, and Justice.[157] An enforcement body would enable OFAC to obtain firsthand information about suspicious activities to supplement potential gaps created by a lack of incentive to self-report[158] or a lack of inter-governmental coordination. This would increase the efficiency and speed of OFAC investigations and enforcement of CISADA. As a result, financial institutions would likely comply more fully with CISADA because of the increased chance in violation detection and punishment.[159] Financial institutions would almost certainly act to avoid civil and criminal penalties and reputational harm that damage their bottom line.[160]

OFAC can use the Department of Commerce's Office of Export Enforcement ("OEE") under the Bureau of Industry and Security as a useful

155 *Cf.* O'Leary, *supra* note 128, at 574-79 (advocating the creation of a National Security Sanctions Court to oversee OFAC designations so OFAC can focus on building evidence against violators).

156 *See supra* note 22 and accompanying text.

157 *See* U.S. DEP'T OF THE TREASURY, *supra* note 20, at 47 (listing collaboration between the U.S. Department of the Treasury and other United States agencies on strategic goals).

158 *See* Fitzgerald, *supra* note 6, at 979-981 (arguing that the lack of highly visible enforcement actions creates an incentive to not comply because it seems unlikely that violations will be enforced).

159 *Cf.* Fitzgerald, *supra* note 6, at 981 (stating that businesses ignore OFAC's regulations because they perceive a low risk of enforcement of violations).

160 *See* Fitzgerald, *supra* note 125 (revealing that financial institutions are reducing business with Iran to avoid reputational harm and fines).

model of an enforcement body.[161] OEE operates in nine United States field offices and employs law enforcement officers to conduct investigations of export violations.[162] In addition, OEE trains agents to conduct site visits to determine the level of risk involved with certain controlled item exports.[163] Like OFAC, OEE utilizes information from a variety of sources, including voluntary self-disclosures of violations.[164] However, OEE's ability to collect its own intelligence and use trained law enforcement officers for compliance makes OEE's enforcement efforts more agile, more direct, and more likely to catch and deter noncompliance than OFAC's near-total reliance on self-disclosures.[165]

An OFAC enforcement body modeled on OEE's site inspection agents would increase direct oversight on compliance programs and procedures under CISADA.[166] OFAC would be better able to review suspicious activity and require the performance of independent audits to satisfy any concerns relating to a United States correspondent banking account with a foreign financial institution.[167] Audits are a critical component of verifying the adequacy of the compliance programs required by CISADA; thus, an enforcement body that could oversee appropriate independent auditing would be extremely useful in advancing CISADA's policy objective of preventing Iranian proliferation.[168] Similarly, an enforcement body would be able to verify certifications that foreign financial institutions were not knowingly engaging in proliferation-related

161 Bureau of Industry and Security, Export Enforcement, http://www.bis.doc.gov/complianceandenforcement/index.htm#oee (last visited on Jan. 13, 2011).

162 *Id.*

163 *Id.*

164 *Id.*

165 *See* Bureau of Industry and Security, *supra* note 161; *supra* note 22 and accompanying text.

166 *See* Comprehensive Iran Sanctions, Accountability, and Divestment Act, 22 U.S.C.A. § 8513 (West 2010); Bureau of Industry and Security, *supra* note 161.

167 *See* Cunningham, *supra* note 140, at 295 (audits provide assurances of compliance).

168 *See* Gregory Husisian, *U.S. Regulation of International Financial Institutions: It's Time for an Integrated Approach to Compliance*, 127 Banking L.J. 195, 198 (2010) (stating that independent auditing is essential to confirm compliance with sanction regulations).

activity.[169] Furthermore, direct oversight of due diligence procedures and internal controls would improve implementation of CISADA[170] while enabling financial institutions to interact more closely with OFAC and enhance the efficacy of their compliance programs.

An OFAC enforcement body that provides effective sanction oversight and enforcement would greatly strengthen CISADA's ability to deter illicit use of correspondent banking in the United States. For instance, the case studies of Barclays, Lloyds, and Credit Suisse suggest that monetary fines and possible damages to corporate reputations are insufficient to deter illicit financial activities with Iranian clients.171 However, if OFAC would continue to aggressively pursue sanction violations by high profile foreign financial institutions through an enforcement body, it would probably win large civil penalty settlements for these violations.[172] As a result, OFAC enforcements would have an increasingly strong deterrent effect on future violations.

The potential precedent set by future cases similar to Barclays, Lloyds, and Credit Suisse would discourage foreign financial institutions from pursuing correspondent banking with the United States on behalf of individuals linked to Iran's WMD program.[173] First, financial institutions would comply with CISADA to protect their profits, especially if they perceive their competitors as being compelled to comply fully with CISADA as well.[174] Second, if the international community continues to agree on the central importance of curtailing Iran's pursuit of WMD, particularly nuclear weapons,[175] the cost of reputational damage if prosecuted for violating CISADA would continue to increase.[176] An

169 *See* 22 U.S.C.A. § 8513(e)(1)(C).

170 *See id.* § 8513(e)(1)(D).

171 *See supra* Part II.

172 *See supra* notes 91-93 and accompanying text.

173 *See supra* notes 91-93 and accompanying text.

174 *See* Fitzgerald, *supra* note 6, at 981.

175 *See supra* note 16.

176 *See* Kittrie, *supra* note 100, at 816-17 (outlining the reputational risk to United States and foreign financial institutions of handling illegitimate business with Iran).

efficient OFAC enforcement body would increase awareness and concern over sanction enforcement among foreign financial institutions with the result being an, increase in CISADA's deterrent effect.[177]

Although a more effective implementation of CISADA would likely cause foreign financial institutions to rethink assistance to Iran's WMD program, foreign financial institutions could simply shift from the United States banking system to other major financial systems in the European Union ("EU") or Asia.[178] However, the use of other systems to avoid United States sanction penalties would probably not be particularly profitable or successful at money laundering or otherwise illicitly funding the Iranian WMD program.[179] Correspondent banking tends to be a concentrated industry due to economies of scale that can be achieved by large-scale correspondent banking practices.[180] In particular, the United States banking system is a large market for correspondent banking accounts due to the United States' importance to international trade and the high demand for the United States dollar.[181]

In addition, a growing international consensus that Iran must be prevented from developing nuclear weapons has resulted in autonomous sanctions from the EU, Canada, and Japan prohibiting correspondent banking accounts with Iranian banks.[182] While none of these sanctions go as

177 *See supra* notes 158-159 and accompanying text.

178 *See* Kittrie, *supra* note 100, at 815 (reporting that many foreign financial institutions have responded to United States' sanctions by terminating business with Iran in United States dollars but not other currencies).

179 *See id.* (stating that most major foreign financial institutions have drastically reduced business with Iran).

180 *See* R. Alton Gilbert, *Economies of Scale in Correspondent Banking*, 15 J. MONEY, CREDIT & BANKING 483 (1983) (explaining that a correspondent bank that services numerous clients experiences economies of scale compared to a smaller correspondent bank because it has greater stability in its balances, which lowers transaction costs when managing its reserve position).

181 *See supra* note 15 and accompanying text.

182 *See* Council Common Position (EC) No. 2007/140/CFSP of 26 July 2010, art.11, L 195/45; Canada Ministry of Foreign Affairs and International Trade, Statement by Minister Cannon on Iran Sanctions, http://www.international.gc.ca/media/aff/news-communiques/2010/237.aspx?lang=eng (last visited on Jan. 13, 2011); Japan Ministry of Foreign Affairs, Accompanying Measures Pursuant to United Nations Security Council Resolution 1929, http://www.mofa.go.jp/region/middle_e/iran/measures_unsc_1009.html

far as CISADA in restricting correspondent banking transactions with any financial institution linked to Iranian proliferation,[183] they represent strong support for the nonproliferation foreign policy goals of the United States.[184] Furthermore, the EU's Third Anti-Money Laundering Directive requires all EU correspondent banking accounts with foreign financial institutions to exercise stringent due diligence requirements,[185] similar to CISADA's enhanced due diligence procedures.[186] This is vital to the success of CISADA because the EU, Canada, and Japan represent significant financial actors in the international banking system outside of the United States. The general support of these countries for financial sanctions to halt Iranian development of a WMD program[187] will likely reduce the ability of foreign financial institutions to evade United States restrictions on correspondent banking by using other major banking systems.

The significant drawback of this proposed enforcement body is its expense, given OFAC's financially strained condition.[188] Although funding is a serious problem, the United States government has repeatedly demonstrated its commitment to combating money laundering and illicit financial activities that support proliferation of WMD.[189] Congress has demonstrated a strong intent to protect United States national security through the implementation of economic sanctions.[190] Therefore, Congress should be willing to invest in a tool that would drastically improve the successful implementation of non-proliferation policies.

(last visited on Jan. 13, 2011).

183 *See* Comprehensive Iran Sanctions, Accountability, and Divestment Act, 22 U.S.C.A. § 8513(c)(1) (West 2010); *supra* note 182 and accompanying text.

184 *See* U.S. DEP'T OF THE TREASURY, *supra* note 20.

185 Council Directive 2005/60/EC, art. 13, ¶ 3, 2005 O.J. (L 309) 25.

186 22 U.S.C.A. § 8513(c)(1)-(2).

187 *See supra* note 182 and accompanying text.

188 Fitzgerald, *supra* note 6, at 962-65.

189 *See* 22 U.S.C.A. §§ 8512-31; Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1114 (1970) (codified as amended at 12 U.S.C. §§ 1829b, 1951-59 (2006) and at 31 U.S.C. §§ 5311-32 (2006)); USA PATRIOT Act, Pub. L. No. 107-56, §§ 301-77, 115 Stat. 272, 296-342 (2001) (codified as amended in scattered sections of U.S.C.).

190 *See* 12 U.S.C. §§ 1829b, 1951-59; 22 U.S.C.A. §§ 8512-31; 31 U.S.C. §§ 5311-32.

In addition, an enforcement body would enjoy some economies of scale from the United States government, which already coordinates with numerous agencies that gather intelligence on terrorism and WMD proliferation.[191] Information sharing would enable the government to reduce costs by synergizing efforts to gather and analyze information. Finally, increased future compliance due to the enhanced capability of the enforcement body to prosecute violations of CISADA would eventually reduce the oversight and prosecution costs of the body.

B. Safe Harbor

OFAC should create a safe harbor clause under CISADA for financial institutions that comply with the statute but make an innocent mistake or technical violation.[192] This clause could be modeled on CISADA's safe harbor clause for insurance underwriters who are exempt from liability for innocent mistakes if they practiced due diligence procedures and controls.[193] An innocent mistake would not constitute a violation of CISADA where (1) the U.S. financial institution had no knowledge that a foreign financial institution was linked to Iran's WMD program; (2) the U.S. financial institution had no bad faith intent to circumvent CISADA; and (3) the facts relating to the foreign financial institution could reasonably be interpreted by the U.S. financial institution to not represent a potential violation of CISADA.[194]

Implementation of CISADA can be very complicated, especially for smaller financial institutions with more limited resources[195] for compliance

---

191 *See supra* note 157 and accompanying text.

192 *See* Fitzgerald, *supra* note 125, at 46 (advocating for a safe harbor from liability for innocent mistakes).

193 COMMITTEE OF CONFERENCE, H.R. COMM. ON FOREIGN AFFAIRS, 111TH CONG., JOINT EXPLANATORY STATEMENT: H.R. 2194, THE COMPREHENSIVE IRAN SANCTIONS, ACCOUNTABILITY, AND DIVESTMENT ACT OF 2010 REPORT, at 12 (2010), *available at* http://www.hcfa.house.gov/111/press_062410d.pdf. The safe harbor sanctions exemption is designed to protect insurance underwriters who use due diligence practices but inadvertently provide insurance for activities that could contribute to Iran's ability to import refined petroleum. *Id.*

194 *See* United States v. N. Pac. Ry. Co., 242 U.S. 190, 194 (1916) (outlining the factors involved in an innocent mistake analysis).

195 *See supra* note 128 and accompanying text.

personnel and software;[196] thus, the odds that an innocent mistake will occur are reasonably high. The complexity of due diligence screening for customer identification information, performing independent audits and certifications, and reporting suspicious activities related to Iranian proliferation efforts is immense, particularly for smaller institutions.[197] In addition, certification that foreign clients are not knowingly engaging in proliferation-related activities and the establishment of due diligence policies under CISADA[198] can be complex and fraught with potential areas for innocent mistakes.

As a result, financial institutions are unlikely to report unintentional violations if the mere act of reporting the violation will result in penalties. A safe harbor clause would improve self-reporting by financial institutions that made an innocent mistake and want to rectify their compliance programs and efforts. Unfortunately, the innocent mistake test that would be applied to the safe harbor clause is imperfect. Specifically, the presumption in favor of a U.S. financial institution's reasonable interpretation of the facts surrounding whether a foreign financial institution is in violation of CISADA is subjective. Nonetheless, the knowledge and bad faith elements can be analyzed objectively based on evidence from the recordkeeping, reporting, and due diligence efforts of the United States financial institution.[199]

C. Clarification

OFAC should also clarify certain terms and how to interpret them to enhance compliance with CISADA. First, OFAC should establish minimal requirements for compliance procedures based on financial institution size[200] and risk assessments of potential financial partners.201 This would

196 *See* MINORITY STAFF OF THE S. PERMANENT SUBCOMM. ON INVESTIGATIONS, 107TH CONG., REP. ON CORRESPONDENT BANKING: A GATEWAY FOR MONEY LAUNDERING, at 1, 11, (2001), *available at* http://hsgac.senate.gov/psi_finalreport.pdf.

197 *See supra* note 128 and accompanying text.

198 22 U.S.C.A. § 8513(e)(1)(C-D).

199 *See* 242 U.S. at 194 (stating that innocent mistakes should be excused based on evidence of good faith).

200 *See* Fitzgerald, *supra* note 125 (explaining that OFAC needs to make the costs of sanction compliance for smaller financial institutions more commercially feasible); *cf.* O'Leary, *supra* note 128 (highlighting that the burden on small charities to ensure the final use of its contributions will not violate sanctions may be too high).

help reduce the burden on small institutions by allowing them to have a more simplified compliance package tailored to their specific needs and limitations.

Second, OFAC should clarify factors that weigh into the materiality of a violation under CISADA and the related penalty scheme. Based on OFAC considerations in previous economic sanction settlements, factors to clarify the materiality of the violation should include: (1) the institutionalization of internal procedures to evade CISADA;[202] (2) the extent of efforts to evade compliance, including omission or removal of information relating to a sanctioned entity;[203] (3) the use of the ordering institution's information instead of the sanctioned entity's name, address, and account; and (4) the use of wire transfer filters to interdict and alter sanctioned entity transactions.[204] The level of penalties associated with these varying degrees of material violations should follow a sliding scale similar to OFAC's settlement determinations. Factors to consider when weighing the penalty to apply should include whether a financial institution voluntarily terminates conduct, cooperates fully with OFAC, and demonstrates good conduct and full compliance in the future.[205] As a result, more explicit guidelines pertaining to the materiality of CISADA violations and the corresponding penalties would likely deter flagrant violations.

It is possible that a sliding scale of penalties based largely on the level of cooperation of offending financial institutions during the settlement process will incentivize some financial institutions to evade sanctions and then present themselves as cooperative upon being caught for violations. However, good faith is implied in all of the elements OFAC considered in

---

201 Special Due Diligence Programs for Certain Foreign Accounts, 72 Fed. Reg. 44,768, 44,769 (Aug. 9, 2007); Special Due Diligence Programs for Certain Foreign Accounts, 71 Fed. Reg. 496, 502 (Jan. 4, 2006); *see also* Fitzgerald, *supra* note 125, at 52-53.

202 Credit Suisse AG, *supra* note 66, at ¶ 13.

203 *Id.* at ¶ 8.

204 Barclays Bank PLC, *supra* note 66, at ¶¶ 7, 8.

205 *See* Barclays Bank PLC, Office of Foreign Assets Control, MUL-488066, (Deferred Prosecution) (Aug. 18, 2010), *available at* http://www.courthousenews.com/2010/08/19/Barclays.pdf (weighing Barclay's violations and remedial actions in determining the details of the settlement agreement); United States v. Credit Suisse AG, No. 1:09-cr-00352-RCL (Deferred Prosecution) (D.D.C. Dec. 16, 2009) (calculating Credit Suisse's violations and remedial actions into the settlement agreement).

the prior enforcement settlements.[206] Furthermore, OFAC can expressly make a showing of good faith a prerequisite for reducing penalties along the sliding scale. Clearer guidelines on materiality and penalty schemes would further deter cheating because financial institutions would be on notice of specific enforceable actions and the pursuant costs.

Finally, OFAC should improve the availability and clarity of information about designated entities, especially contact and account information, for financial institutions to confirm whether an actor is designated as being linked to Iran's WMD program.[207] Increased publication of information about actors linked to Iranian proliferation through designation lists on the OFAC website would help prevent financial institution violations of CISADA and provide an affirmative conveyance of "knowledge" to trigger prosecution of any violations.[208] A possible model to increase the availability of information about actors linked to Iranian proliferation is the Treasury's Weekly Bulletin Search in the Office of the Comptroller of the Currency.[209] Creating a similar "bulletin" with information about mergers, addresses, branches, subsidies, and certifications for foreign financial institutions would substantially improve the ability of United States financial institutions to evaluate the risk of a potential correspondent banking client abroad.[210] This would help financial institutions to comply more accurately with CISADA while also allowing OFAC to share information about new front companies or other means of evasion that certain actors are currently utilizing to access the United States financial system.

206 *Id.*

207 Fitzgerald, *supra* note 125, at 41, 44.

208 *See* Fitzgerald, *Pierre Goes Online: Blacklisting and Secondary Boycotts in U.S. Trade Policy*, 31 VAND. J. TRANSNAT'L L. 1, 33 (1998) (affirming that a government declaration that an actor is linked to Iranian proliferation conveys affirmative knowledge about sanction violations).

209 Office of the Comptroller of the Currency, Weekly Bulletin Search, http://www.occ.gov/tools-forms/tools/licensing/weekly-bulletin-corp-apps-search.html (last accessed on Jan. 13, 2011).

210 *See id.*

Conclusion

CISADA represents a cumulative effort by the United States to prevent money laundering and illicit transactions that endanger United States national security.[211] Unfortunately, the overall effectiveness of this statute and its compliance tools remains unclear. CISADA relies heavily on self-reporting, including user certifications based on the best knowledge of United States financial institutions,[212] which may be deceived by ever-shifting front companies and evasive measures by Iran. Due diligence and audits for correspondent banking with foreign financial institutions may not be sufficient to protect against industrious Iranian actors.[213] Instead, OFAC needs to create an enforcement body to investigate potential violations, expressly include a safe harbor clause for innocent mistakes, and codify factors relating to materiality of violations and corresponding penalty schemes in order to increase compliance with CISADA. By reducing the burden of compliance for financial institutions and increasing the risk of being prosecuted for violations, OFAC can improve compliance with CISADA through clearer regulations and increased information sharing. In doing so, OFAC would protect more strongly the foreign policy objectives of the United States, including the prohibition of proliferator access to the United States banking system to pay for WMD-related components.[214]

211 *See* 22 U.S.C.A. §§ 8512-31 (West 2010); *supra* notes 20, 25, 36 and accompanying text.

212 Comprehensive Iran Sanctions, Accountability, and Divestment Act, 22 U.S.C.A. § 8513(e)(1)(B-C) (West 2010).

213 *Id.* § 8513(e)(1)(A)(D).

214 U.S. DEP'T OF THE TREASURY, *supra* note 20.