UNIVERSITY *of* PENNSYLVANIA LAW REVIEW

Founded 1852

Formerly
AMERICAN LAW REGISTER

VOL. 162 FEBRUARY 2014 NO. 3

ARTICLE

FUNDING TERROR

SHIMA BARADARAN,[†] MICHAEL FINDLEY,[‡] DANIEL NIELSON[††] & JASON SHARMAN[‡‡]

[†] Associate Professor of Law, University of Utah College of Law. We thank the Yale University Institution for Social and Policy Studies (ISPS) for their support of this project and the BYU Office of Research & Creative Activities for their award of a MEG Grant in support and furtherance of our work. We express gratitude to the Yale, Columbia, Cornell, Maryland, Northwestern, Vanderbilt, William & Mary, Utah, University of Miami, Wisconsin, USC, and BYU law and political science faculties for their feedback. We would also like to thank officials in the U.S. Department of Justice, Internal Revenue Service, Financial Action Task Force (FATF), World Bank, International Monetary Fund (IMF), Senate Permanent Subcommittee on Investigations, and United Nations Office on Drugs and Crime for their assistance in this project. Special thanks to Spencer Driscoll as a student contributor on this Article. We express gratitude to Professors Oona Hathaway, Jack Goldsmith, Eric Posner, Jide Nzelibe, Susan Hyde, Robert Keohane, Daniel Kono, Jim Kuklinski, Larry May, Robert Mikos, David Moore, David Gray, Dan Goldberg, Bill Reynolds, Max Sterns, Stephanie Rickard, Toby Rider, Michael A. Newton, Christopher Slobogin, Scott Wolford, Ingrid Wuerth, Yesha Yadav, Carissa Hessick, Scott Dodson, and Thomas Nance for their extremely useful comments.

The events of September 11, 2001, forever changed the political and legal responses to terrorism. After more than ten years, two wars, numerous targeted military strikes, and significantly increased surveillance, we have not stopped the growth of al-Qaeda and other terrorist organizations. The War on Terror has involved more than military operations. To stop terrorism, it is imperative to cut off its funding stream. To this end, a number of nations have created financial laws that prohibit the formation of anonymous companies and monitor suspicious bank transfers. Though these laws have been touted as evidence that we are winning the War on Terror, this Article questions their efficacy. In particular, this Article demonstrates how easy it is to form a terrorist finance network and to exploit the impotence of these international and domestic financial regulations. The Article presents findings from the largest global, randomized controlled trial on this issue to date. In our experiment, we acted as customers seeking to form anonymous shell companies in a variety of scenarios resulting in either greater risk or greater reward. On the whole, forming an anonymous shell company is as easy as ever, despite increased regulations following September 11. The results are disconcerting and demonstrate that we are far from a world that is safe from terror.

The research design for this experiment was registered on March 2, 2011, with ISPS, prior to the beginning of the Experiments in Governance and Politics (EGAP) registry but was grandfathered into EGAP later. Registration pages for ISPS and EGAP, respectively, are at http://isps.yale.edu/research/projects/p11-001#.UT39V9F4ZxF and http://e-gap.org/wp/wp-content/uploads/20110302_NFSB_Compliance.pdf. Of those interventions registered, we report on the Placebo, Terrorism, FATF, and IRS conditions in this Article. All other interventions outlined in the registered document are reported in other work. In our registration, we indicated that we would report results dichotomously as compliant or noncompliant, given a response. In this Article, we still report response and nonresponse along with a compliance level, but we expanded the set of possible types of compliance (nonresponse, noncompliance, partial compliance, compliance, and refusal). Presenting the information this way is both more precise and consistent with the registry document because the fuller set of outcomes contains all information the dichotomized measures capture. University and Institutional Review Board Clearances were received on July 7, 2010.

‡ Assistant Professor of Government, University of Texas at Austin.

††Associate Professor of Political Science, Brigham Young University.

‡‡ Professor of Political Science, Center for Governance and Public Policy, Griffith University, Australia.

INTRODUCTION

Financing—particularly, a secure financing network—is crucial for terror organizations.[1] To finance its international operations, al-Qaeda requires an estimated $30–$50 million per year.[2] Establishing al-Qaeda's financing network was one of Osama bin Laden's earliest and most important accomplishments[3] because it provided millions in "steady and secure" income to the organization.[4] Not every act of terrorism, however, requires terrorist organizations to spend great sums of money. For instance, the September 11 attacks cost al-Qaeda approximately $400,000–$500,000,[5] but "[t]he London transit bombings on July 7, 2005, only cost about $15,000."[6] Because terrorists

1 In a 2007 interview, former al-Qaeda Chief Treasurer Sheik Saeed declared that "funding is the mainstay of jihad." Ari Shapiro, *Morning Edition: Obama Stays the Course on Terrorist Financing* (NPR radio broadcast Mar. 11, 2009, 12:17 AM), *available at* http://www.npr.org/templates/story/story.php?storyId=101676777.

2 JIMMY GURULÉ, UNFUNDING TERROR: THE LEGAL RESPONSE TO THE FINANCING OF GLOBAL TERRORISM 3 (2008); NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 169-72 (2004) [hereinafter 9/11 COMMISSION REPORT], *available at* http://www.9-11commission.gov/report/911Report.pdf; *see also* NICK RIDLEY, TERRORIST FINANCING: THE FAILURE OF COUNTER MEASURES 1-2 (2012) ("[E]fforts against terrorist financing tend to be focused on assessing and calculating individual operational costs, and the significance of auxiliary support or infrastructure is not yet fully apparent to organizations and agencies engaged in counter terrorism.").

3 *See* INDEP. TASK FORCE, COUNCIL ON FOREIGN RELATIONS, TERRORIST FINANCING 6 (2002) [hereinafter CFR, TERRORIST FINANCING], *available at* http://www.cfr.org/terrorist-financing/terrorist-financing/p5080 (explaining that al-Qaeda is difficult to attack, in part because it is "continuously replenishing its coffers").

4 JOHN ROTH ET AL., NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, MONOGRAPH ON TERRORIST FINANCING: STAFF REPORT TO THE COMMISSION 30 (2004), *available at* http://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Monograph.pdf.

5 9/11 COMMISSION REPORT, *supra* note 2, at 169; *see also* ROTH ET AL., *supra* note 4, at 13 (noting further that of that sum, "approximately $300,000 was deposited into U.S. bank accounts of the 19 hijackers").

6 Greg Bruno, *Al-Qaeda's Financial Pressures*, COUNCIL ON FOREIGN RELATIONS (Feb. 1, 2010), http://www.cfr.org/terrorist-organizations/al-qaedas-financial-pressures/p21347; *cf.* Michael Buchanan, *London Bombs Cost Just Hundreds*, BBC NEWS (Jan. 3, 2006), http://news.bbc.co.uk/2/hi/uk/4576346.stm (estimating that the attacks cost only several hundred British pounds).

can accomplish enormously destructive attacks with very little money, a successful war on terror must reach deep into the financial heart of terrorism.

Though terror attacks are often inexpensive, the efforts to prevent them are not. To combat terrorism and drain the pipeline of funds, the United States has frozen al-Qaeda's U.S. assets[7] and spent more than $1.2 trillion since 9/11 on its major military and diplomatic operations abroad, as well as "medical care for Iraq and Afghan war veterans."[8] The overall costs of fighting terrorism have compounded the national deficit[9] and greatly impacted the financial markets.[10] One group of commentators has even called this fight the "three trillion dollar war."[11] This is not to mention the other costs of terrorism, including the cost to civil liberties of security measures.[12] Terrorism's financial impact reaches far beyond U.S. borders; other

---

7 David L. Greene, *U.S. Freezes bin Laden Assets*, BALT. SUN, Sept. 25, 2001, at 1A.

8 AMY BELASCO, CONG. RESEARCH SERV., RL33110, THE COST OF IRAQ, AFGHANISTAN, AND OTHER GLOBAL WAR ON TERROR OPERATIONS SINCE 9/11, at 1 (2011).

9 Jacqueline Leo, *Bin Laden Cost U.S. Trillions, Affecting Deficit*, FISCAL TIMES (May 2, 2011), http://www.thefiscaltimes.com/Articles/2011/05/02/Bin-Laden-Cost-US-Trillions-Affecting-Deficit; *see also* JOHN MUELLER & MARK STEWART, TERROR, SECURITY, AND MONEY: BALANCING THE RISKS, BENEFITS, AND COSTS OF HOMELAND SECURITY 3 (2011) (estimating the enhanced costs of homeland security in the decade after 9/11 at more than $1 trillion).

10 *See* Michael J. Mandel et al., *The Cost of Fighting Terrorism*, BUSINESSWEEK, Sept. 16, 2002, at 26 ("[B]oth the stock market and the labor market are weaker than they were before September 11 . . . .").

11 JOSEPH E. STIGLITZ & LINDA J. BILMES, THE THREE TRILLION DOLLAR WAR: THE TRUE COST OF THE IRAQ CONFLICT (2008); *see also* Linda J. Bilmes & Joseph E. Stiglitz, Op-Ed., *America's Costly War Machine*, L.A. TIMES (Sept. 18, 2011), http://articles.latimes.com/2011/sep/18/opinion/la-oe--bilmes-war-cost-20110918 ("[T]he United States has spent more than $2.5 trillion on the wars in Iraq and Afghanistan . . . .").

12 *See, e.g.*, DAVID COLE, ENEMY ALIENS 72-75 (2003) (discussing proposed security programs that would endanger civil liberties, such as the Terrorist Information and Protection System that would enlist private citizens to spy on their neighbors); DAVID COLE & JAMES X. DEMPSEY, TERRORISM AND THE CONSTITUTION: SACRIFICING CIVIL LIBERTIES IN THE NAME OF NATIONAL SECURITY 147-76 (2002) (finding that the expansion of law enforcement powers of the Anti-Terrorism Act of 1996 through the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of the U.S.C.), "reflects an overreaction all too typical in American history[,] . . . cast[ing] a cloak over the exercise of government power by removing limitations and judicial controls on investigative authorities, and short-circuit[ing] procedures designed to protect the innocent and punish the guilty"); Norman C. Bay, *Executive Power and the War on Terror*, 83 DENV. U. L. REV. 335, 370-71 (2005) (expressing concern over the effect the "blur[ring of] the line between a military and law enforcement response to terrorism" has on civil liberties); Erwin Chemerinsky, *Civil Liberties and the War on Terrorism*, 45 WASHBURN L.J. 1, 2-14 (2005) (discussing detention of individuals without due process and other costs imposed on civil liberties by the PATRIOT Act); Christopher Edley, Jr., *The New American Dilemma: Racial Profiling Post-9/11* (describing the spread of racial profiling after September 11), *in* THE WAR ON OUR FREEDOMS: CIVIL LIBERTIES IN AN AGE OF TERRORISM 170, 170-74 (Richard C. Leone & Greg Anrig, Jr., eds., 2003); Wendy Pollack, *The True Cost of*

nations have also spent billions of dollars combating it.[13] The United Kingdom, for instance, spends an estimated £3.5 billion per year to fight terrorism.[14]

Though the United States has spent enormous sums to fight terrorism with its military might, many are concerned that it has not invested sufficient resources in cutting off the true lifeline of terrorism: its clandestine network of global financing.[15] As this Article examines in great detail, one of the most dangerous and accessible financial tools used by terrorists today is the anonymous shell company.[16] These companies allow terrorists to disguise their identities and covertly transfer funds—even within U.S. banks—toward illegal activities. Shell companies pose particularly vexing problems for law enforcement because there is often no way to trace them to individuals.[17] The

Fighting Terrorism, WALL ST. J. BLOGS: THE INFORMED READER (Sept. 21, 2007), http://blogs.wsj.com/informedreader/2007/09/21/the-true-cost-of-fighting-terrorism ("The Sept. 11 attacks have encouraged democracies to tolerate physical abuse of suspected terrorists . . . .").

13 *See, e.g.*, Tom Hyland, *Terror Fight Costs $30 Billion*, AGE (Sept. 11, 2011), http://www.theage.com.au/national/terror-fight-costs-30-billion-20110910-1k3ez.html (estimating that Australia has spent nearly $30 billion fighting terrorism since 9/11).

14 Andy McSmith, *Home Office: Cost of Fighting Terrorism Triples to £3.5bn by 2010*, INDEPENDENT (Oct. 10, 2007), http://www.independent.co.uk/news/uk/politics/home-office-cost-of-fighting-terrorism-triples-to-pound35bn-by-2010-396473.html.

15 *See, e.g.*, CFR, TERRORIST FINANCING, *supra* note 3, at 2-3 ("[T]he current administration appears to have made a policy decision not to use the full power of U.S. influence to pressure or compel other governments to combat terrorist financing more effectively."); RAPHAEL PERL, CONG. RESEARCH SERV., RL33160, COMBATING TERRORISM: THE CHALLENGE OF MEASURING EFFECTIVENESS 2-3 (2007) (noting that even the seizure of terrorist funds may not indicate progress toward eradicating terrorism, since this may not affect the terrorists' ability to raise additional financing for expansion); MARTIN A. WEISS, CONG. RESEARCH SERV., RS21902, TERRORIST FINANCING: THE 9/11 COMMISSION RECOMMENDATION 1-2 (2004) ("The slowdown in the amounts frozen reflects numerous changes in how Al Qaeda and other terrorist groups finance their activities. Terrorist organizations are increasingly relying on informal methods of money transfer, and regional cells have begun independently generating funds through criminal activity."); Michael Jacobson & Matthew Levitt, *Staying Solvent: Assessing Al-Qaeda's Financial Portfolio*, JANE'S STRATEGIC ADVISORY SERVS., Nov. 2009, at 9, 12-13 ("Al-Qaeda has at times also resorted to more creative means of fundraising, including complicated internet-based transactions and cell phone solicitations.").

16 *See, e.g.*, FED. FIN. INSTS. EXAMINATION COUNCIL, BANK SECRECY ACT/ANTI–MONEY LAUNDERING EXAMINATION MANUAL, app. F at F-1 (2010), *available at* http://www.ffiec.gov/bsa_aml_infobase/documents/bsa_aml_man_2010.pdf (listing shell companies as a "red flag" for terrorist financing); FIN. CRIMES ENFORCEMENT NETWORK, THE ROLE OF DOMESTIC SHELL COMPANIES IN FINANCIAL CRIME AND MONEY LAUNDERING: LIMITED LIABILITY COMPANIES 11-13 (2006), *available at* http://www.fincen.gov/news_room/rp/files/LLCAssessment_FINAL.pdf (pointing out that the lack of adequate legal reporting requirements for LLCs contributes to their continued success as shell companies that facilitate illegal activity); *They Sell Sea Shells*, ECONOMIST, Apr. 7, 2012, at 69, 69 (noting that, despite their legitimate uses, shell companies "can also be misused—for tax evasion, money laundering, sanctions-busting or terrorism").

17 *See, e.g.*, EMILE VAN DER DOES DE WILLEBOIS ET AL., STOLEN ASSET RECOVERY INITIATIVE, THE PUPPET MASTERS: HOW THE CORRUPT USE LEGAL STRUCTURES TO

only tangible component of a shell company may be a post office box; in other words, shell corporations are often "hollow" companies.[18] Shell corporations can serve some legitimate purposes, such as facilitating mergers, enabling international joint ventures, and serving as asset-holding companies.[19] However, because they are "hollow," they are commonly used as vehicles for corruption, money laundering, and, more recently, terrorism. Although many of these organizations seem harmless when they are created, posing as charities or legitimate businesses, they often become involved in illicit activities and frequently lead law enforcement investigations to dead ends.[20] In an effort to combat terrorist financing, policymakers have begun identifying vulnerabilities in financial institutions and the ways in which terrorists have exploited them.[21] New legislation has pushed for financial

---

HIDE STOLEN ASSETS AND WHAT TO DO ABOUT IT 38-39 (2011) [hereinafter PUPPET MASTERS], *available at* http://elibrary.worldbank.org/doi/pdf/10.1596/978-0-8213-8894-5 (noting that the owners of a shelf corporation, a form of shell company, can be untraceable if ownership is never officially transferred by registering with the proper authorities); Richard K. Gordon, *Trysts or Terrorists? Financial Institutions and the Search for Bad Guys*, 43 WAKE FOREST L. REV. 699, 726-28, 735-36 (2008) (explaining that financial institutions use very rough "typologies" to determine which transactions present a higher risk of laundering, and that even when such transactions are identified, there is little guidance "to make clear how far a financial institution should go to identify clients"); J.W. Verret, *Terrorism Finance, Business Associations, and the "Incorporation Transparency Act*," 70 LA. L. REV. 857, 857-58, 909-10 (2010) (recognizing the law enforcement problems posed by the lack of mandatory company ownership reporting, but noting that the Incorporation Transparency and Law Enforcement Assistance Act is little more than "an empty gesture meant to generate the appearance of action"); Stefanie Ostfeld, *Shell Game: Hidden Owners and Motives*, CNN (Sept. 11, 2012), http://www.cnn.com/2011/10/26/opinion/ostfeld-shell-companies/index.html ("The same loophole that allowed a donor to hide behind an anonymous shell company provides terrorists, corrupt foreign politicians and drug traffickers opportunity to squirrel dirty money into and through the U.S. financial system.").

18 *See* PUPPET MASTERS, *supra* note 17, at 35 (describing shell companies as "hollow" because they are nonoperational as a corporate structure, although they can be used for legitimate legal purposes).

19 *Id. But see* David Spencer, *International Tax Evasion: Enablers and Shell Corporations* (pt. 2), J. INT'L TAX'N, May 2007, at 36, 38 (noting that some companies "have used more sophisticated cross-border schemes and/or investment structures . . . which go beyond legitimate tax minimization arrangements"); Robert Paul Turner, *The Death of the Shell Game*, NEV. LAW., Jan. 2002, at 7, 7 (noting a severe decline in the use of shell companies as fronts for mergers).

20 *See* PUPPET MASTERS, *supra* note 17, at ix ("Law enforcement and prosecution cannot go after stolen assets, confiscate and then return them if they are hidden behind the corporate veil."); Dean Kalant, *Who's in Charge Here? Requiring More Transparency in Corporate America: Advancements in Beneficial Ownership for Privately Held Companies*, 42 J. MARSHALL L. REV. 1049, 1050 (2009) (noting that "a person forming a corporation or LLC within the United States typically is required to 'provide less information to the state of incorporation than is needed to obtain a bank account or driver's license,'" resulting in an "extreme lack of ownership transparency in the United States").

21 *See, e.g.*, *U.S. Vulnerabilities to Money Laundering, Drugs, and Terrorist Financing: HSBC Case History: Hearing Before the Permanent Subcomm. on Investigations of the S. Comm. on Homeland Sec. & Gov't Affairs.*, 112th Cong. 2-3 (2012) (statement of David S. Cohen, Undersecretary for Terrorism

transparency as a way to avoid corruption and obstruct terrorist financing both within the United States and globally,[22] but the effectiveness of these efforts is debatable, given terrorist organizations' ability to adapt quickly.[23] While others have commented about how easy it is to form anonymous shell companies,[24] no study thus far has determined how effective domestic and international regulations have been at curbing their proliferation and use.[25]

---

and Fin. Intelligence, Dep't of the Treasury) (providing case studies detailing the manner in which terrorist organizations have taken advantage of weaknesses in the U.S. financial system for illicit activities); WORLD BANK, COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM: A COMPREHENSIVE TRAINING GUIDE 13 (2009) (listing examples of businesses that are particularly vulnerable to terrorist financing).

22 *See, e.g.*, Bank Secrecy Act of 1970, 12 U.S.C. § 1829b (2012) (imposing mandatory record-keeping requirements on financial institutions with penalties for noncompliance); Money Laundering Control Act of 1986, 18 U.S.C. §§ 1956–1957 (2006 & Supp. V 2012) (imposing criminal penalties for money laundering); Suppression of the Financing of Terrorism Convention Implementation Act of 2002, 18 U.S.C. § 2339C (2006) (making the financing of terrorism a punishable federal offense); International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001, 31 U.S.C. § 5311 (2006) (criminalizing the acts of financing terrorism, increasing scrutiny of transactions with foreign shell companies, and adopting other measures to prevent money laundering); Money Laundering and Financial Crimes Strategy Act of 1998, 31 U.S.C §§ 5340–5355 (2006) (designating high-risk areas for money laundering and related financial crimes); International Emergency Economic Powers Act of 1977, 50 U.S.C. §§ 1701–1707 (2006 & Supp. V 2012) (providing executive power to intervene in foreign conflicts using financial means); Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 6101, 118 Stat. 33638 (codified as amended in scattered sections of the U.S.C.) (authorizing expenditures for technology to prevent financial crimes and terrorism in the United States); Money Laundering Suppression Act of 1994, Pub. L. No. 103-325, tit. IV, 108 Stat. 2160 (codified as amended in scattered sections of 31 U.S.C.); Annunzio–Wylie Anti–Money Laundering Act of 1992, Pub. L. No. 102-550, tit. XV, 106 Stat. 4044 (codified as amended in scattered sections of 31 U.S.C.) (authorizing the revocation of various privileges of financial institutions convicted of money laundering). For commentary on interagency coordination to curb terrorist financing, see generally WEISS, *supra* note 15.

23 *See* 9/11 COMMISSION REPORT, *supra* note 2, at 169 ("The plotters' tradecraft was not especially sophisticated, but it was good enough. They moved, stored, and spent their money in ordinary ways, easily defeating the detection mechanisms in place at the time."); U.S. GEN. ACCOUNTING OFFICE, GAO-04-163, TERRORIST FINANCING: U.S. AGENCIES SHOULD SYSTEMATICALLY ASSESS TERRORISTS' USE OF ALTERNATIVE FINANCING MECHANISMS 9 (2003) ("To move assets, terrorists use mechanisms that enable them to conceal or launder their assets through nontransparent trade or financial transactions such as charities, informal banking systems, bulk cash, and commodities such as precious stones and metals."); Jacobson & Levitt, *supra* note 15, at 13 ("Due to the increased international scrutiny, Al-Qaeda has also become far more security conscious in its fundraising activities.").

24 *See generally* J.C. SHARMAN, THE MONEY LAUNDRY: REGULATING CRIMINAL FINANCE IN THE GLOBAL ECONOMY (2011); PUPPET MASTERS, *supra* note 17 (detailing the relative ease with which illicit activity can be conducted using legitimate corporate forms); Chana Joffe-Walt, *Morning Edition: We Set Up an Offshore Company in a Tax Haven* (NPR radio broadcast July 27, 2012, 5:00 AM), *available at* http://www.npr.org/blogs/money/2012/07/27/157421340/how-to-set-up-an-offshore-company (discussing businesses that inexpensively set up secret offshore companies for their clients); Kevin McCoy, *Project Shows Ease of Money Laundering in USA*, USA

This Article and the experiment we developed seek to fill this void and measure the effectiveness of domestic and international law at curbing the use of shell companies. Because the United States spends billions of dollars each year on counterterrorism, understanding the effectiveness of these efforts is crucial.[26] Measuring their effectiveness is increasingly difficult, and much of the rhetoric concerning successful U.S. intervention into the terrorism-financing network is simply political.[27] Policymakers often offer "perceptions of success" without providing data or even explaining their methodology.[28] This Article seeks to move the discussion forward by delivering extensive empirical data on the effectiveness of worldwide efforts to curb terrorist financing.

The Article is divided into three parts. Part I outlines the current financial tools at terrorists' disposal. It pays particular attention to anonymous shell companies and discusses the laws intended to stop the formation of such companies, their shortcomings, and other countervailing domestic policies and case law that foster their use. It then discusses the steps taken by the United States and the international community after 9/11 to reduce the threat of terrorism.

TODAY (Mar. 19, 2007), http://www.usatoday.com/money/companies/2007-03-19-money-launder-usat_N.htm (describing a project in which retired IRS agents very easily set up secretive companies and transferred money between them).

25 While this Article takes a more empirical approach, the Council on Foreign Relations' Independent Task Force provides a policy critique of the United States' post-9/11 efforts in this area. *See generally* CFR, TERRORIST FINANCING, *supra* note 3.

26 For differing perspectives on the effectiveness of U.S. efforts to fight terrorism through financial regulation, see AVI JORISCH, TAINTED MONEY: ARE WE LOSING THE WAR ON MONEY LAUNDERING AND TERRORISM FINANCING? 131-36 (2009); PERL, *supra* note 15; PAUL ROGERS, WHY WE'RE LOSING THE WAR ON TERROR 146-49 (2008); Jacobson & Levitt, Op-Ed., *Staying Solvent: Assessing Al-Qaeda's Financial Portfolio*, WASH. INST., Nov. 2009, at 9, 12, *available at* http://www.washingtoninstitute.org/uploads/Documents/opeds/4b28f9a9e2216.pdf; Ahmed Rashid, *Losing the War on Terror*, WASH. POST, Sept. 11, 2006, at A17; Press Release, U.S. Dep't of the Treasury, Assistant Secretary for Terrorist Financing David S. Cohen Remarks to the ABA/ABA Money Laundering Enforcement Conference (Oct. 12, 2009), *available at* http://www.treasury.gov/press-center/press-releases/Pages/tg317.aspx.

27 *See* Sue E. Eckert & Thomas J. Biersteker, *(Mis)Measuring Success in Countering the Financing of Terrorism* (describing the political utility of countering the financing of terrorism, and crediting that utility with politicizing the numbers and rhetoric surrounding terrorist financing), *in* SEX, DRUGS, AND BODY COUNTS: THE POLITICS OF NUMBERS IN GLOBAL CRIME AND CONFLICT 247, 247-49 (Peter Andreas & Kelly M. Greenhill eds., 2010). Eckert and Biersteker note that while "there are no definitive metrics by which success or effectiveness can be assessed" in this domain, there is still "a variety of information and indicators that can help paint an overall picture." *Id.* at 260. They also argue that effectiveness can be difficult to measure because much of the valuable information and data is classified. *Id.* at 258.

28 *See id.* at 256 (critiquing the Bush Administration for failing to explain its metrics for claiming counterterrorism success).

Part II describes and analyzes the results from our experiment, in which we posed as customers from around the globe seeking to form anonymous shell companies.[29] During the course of our study, we sent more than 7400 requests to service providers worldwide asking for their assistance in forming anonymous shell companies. In some requests, we included obvious indicators of terrorism risk. In others, we tested whether knowledge of international standards set by the Financial Action Task Force (FATF) and the IRS would impact the number of offers we received. Overall, as described below, the results were disconcerting. In particular, knowledge of international law proved much less of a deterrent to forming shell companies than one might hope. Indeed, our results suggest that these financial regulations may not be effective constraints on funding terrorism.

Part III uses these results to answer some important questions. For instance, are certain countries or blocs of countries more likely to form fronts for terrorism? Do offshore states (i.e., tax havens) allow anonymous companies to form more easily? Are poor countries more likely than rich countries to facilitate terrorism financing? Is domestic or international law a more successful deterrent to the formation of shell companies in the United States? This Article concludes with some important lessons that can help U.S. regulators and the international community undermine financial support for terrorists and mitigate the threat of future terrorism.

I. THE DOMESTIC AND INTERNATIONAL WAR ON TERROR

In the days following the September 11 attacks, the United States took immediate steps to secure its borders, engage its military, and expand the scope of its intelligence efforts.[30] As previously noted, some analysts estimate that fighting the War on Terror has cost the United States more than $3 trillion.[31] Though the United States' response to the attacks is not

---

[29] The full experiment is discussed in MICHAEL G. FINDLEY, DANIEL L. NIELSON, & J.C. SHARMAN, GLOBAL SHELL GAMES: EXPERIMENTS IN TRANSNATIONAL RELATIONS, CRIME, AND TERRORISM (2014). On the need for experiments in international law more generally, see Adam Chilton & Dustin Tingley, *Why the Study of International Law Needs Experiments* 52 Colum. J. Transnat'l L. 173 (2014).

[30] *See* 9/11 COMMISSION REPORT, *supra* note 2, at 330-38 (providing a detailed account of the days following and the United States' military response to the September 11 attacks); Amy B. Zegart, *September 11 and the Adaptation Failure of U.S. Intelligence Agencies*, INT'L SEC., Spring 2005, at 78, 107-11 (describing the U.S. intelligence community's responses and failures after 9/11).

[31] *E.g.*, Shan Carter & Amanda Cox, *One 9/11 Tally: $3.3 Trillion*, N.Y. TIMES (Sept. 8, 2011), http://www.nytimes.com/interactive/2011/09/08/us/sept-11-reckoning/cost-graphic.html.

without its failings,[32] its military and intelligence communities responded swiftly to disrupt terrorist activity at home and abroad.[33] The United States has also taken steps "to target aggressively Islamic terrorism's financial infrastructure."[34] These efforts spanned the globe, as the United States reached out to other nations and organizations to assist in achieving its goal of preventing terrorism financing in domestic and world markets.[35] But as the United States worked to dismantle terrorist financing networks, terrorists adapted. To preserve their cash flow, they have resorted to more clandestine sources of funding.[36] Because the United States has been slow to respond, it has been criticized as "lack[ing] the same creativity and innovation that al-Qaeda financiers use each day in their planning."[37]

This Part examines the "creative" tools that terrorists use to finance their operations, focusing on shell companies. It then summarizes domestic and international responses to the threat of terrorist financing, and compares U.S. efforts with those of the international community. Finally, it parses out the shortcomings of those policies and describes how domestic policies might actually be promoting and furthering the use of shell companies as a front for terrorism and other illicit activities.

---

32 *See* John Mueller & Mark G. Stewart, *The Terrorism Delusion: America's Overwrought Response to September 11*, INT'L SEC., Summer 2012, at 81, 95-107 (describing how disproportionate and costly America's response has been to al-Qaeda compared to the actual threat that al-Qaeda poses).

33 *See* U.S. DEP'T OF HOMELAND SEC., IMPLEMENTING 9/11 COMMISSION RECOMMENDATIONS: PROGRESS REPORT 2011, at 43 (2011) (detailing the Department of Homeland Security's progress in implementing the recommendations of the 9/11 Commission, including the Commission's recommendation to track and disrupt terrorist financing); Stewart M. Patrick, *The Unsung Success After 9/11: Multilateral Cooperation*, INTERNATIONALIST (Sept. 6, 2011), http://blogs.cfr.org/patrick/2011/09/06/the-unsung-success-after-911-multilateral-cooperation (cataloging the unprecedented international collaboration that followed 9/11); *Ten Years After: The FBI Since 9/11*, FBI, http://www.fbi.gov/about-us/ten-years-after-the-fbi-since-9-11/response-and-recovery (detailing the FBI's response in the aftermath of 9/11) (last visited Jan. 24, 2014). *See generally* Jena Baker McNeill et al., *39 Terror Plots Foiled Since 9/11: Examining Counterterrorism's Success Stories*, BACKGROUNDER (Heritage Found., Phila., Pa.), May 20, 2011, at 1, *available at* http://www.heritage.org/research/reports/2011/05/39-terror-plots-foiled-since-911-examining-counterterrorisms-success-stories.

34 CFR, TERRORIST FINANCING, *supra* note 3, at 12. The Council on Foreign Relations identified three tactical decisions taken by the Bush Administration after September 11, including increased intelligence activities, law enforcement coordination, and "public designations under the International Emergency Economic Powers Act (IEEPA) [to block certain] persons, businesses, and financial institutions" from furthering terrorism. *Id.* The Council also identified strategic initiatives adopted by the Bush Administration and Congress, such as legislation like "sweeping new anti–money laundering laws" and the PATRIOT Act, as well as multilateral initiatives involving the United Nations, the International Monetary Fund (IMF), the World Bank, and the FATF. *Id.* at 13-14.

35 *Id.* at 13.

36 *See supra* note 15 and accompanying text.

37 CFR, TERRORIST FINANCING, *supra* note 3, at 32.

A. *Financial Tools at Terrorists' Disposal*

Terrorists use a variety of financial tools to fund their activities, including money laundering, charities, trusts, and, most notably, shell companies.

1. Money Laundering

Terrorists rely on money laundering to avoid detection.[38] Money laundering is a multi-layered process by which terrorists hide the illegal source or use of income and then "disguise[] that income to make it appear legitimate."[39] It is estimated that between $590 billion and $1.5 trillion is laundered annually worldwide, and some of that money is used to fund terrorist organizations.[40] Money laundering happens in three basic stages: placement, layering, and integration.[41] During the placement stage, money obtained from illegal practices is deposited into a financial institution.[42] The layering stage occurs when the money is "pass[ed] . . . through many institutions and jurisdictions," which aids in covering up the illegal source of the funds.[43] Shell companies are important to this stage of the process because the layering transactions involve moving funds to supposedly legitimate companies.[44] Finally, during the integration stage, money is put back into the economy "through normal financial or commercial operations" in a way that makes it appear legitimate.[45] Informal Value Transfer Systems (IVTS), which are used heavily in the Middle East and Asia, are of particular concern

---

38 *See, e.g.*, Amos N. Guiora & Brian J. Field, *Using and Abusing the Financial Markets: Money Laundering as the Achilles' Heel of Terrorism*, 29 U. PA. J. INT'L L. 59, 59-61 (2007) (arguing that undermining the ability of financiers of terrorism to launder money is critical to combating terrorists). Terrorists finance their activities through a variety of illegal activities, including "extortion, kidnapping, narcotics trafficking, counterfeiting, and fraud," but the money from those activities often needs to be laundered before it can move into terrorists' hands. *Terrorism: Growing Wahhabi Influence in the United States: Hearing Before the Subcomm. on Terrorism, Tech. and Homeland Sec. of the S. Comm. on the Judiciary*, 108th Cong. 68 (2003) (statement of David D. Aufhauser, Gen. Counsel, Dep't of the Treasury).

39 Lisa A. Barbot, *Money Laundering: An International Challenge*, 3 TUL. J. INT'L & COMP. L. 162, 162 (1994); *see also* Alison S. Bachus, Note, *From Drugs to Terrorism: The Focus Shifts in the International Fight Against Money Laundering After September 11, 2001*, 21 ARIZ. J. INT'L & COMP. L. 835, 835 (2004).

40 *What Is Money Laundering?*, FATF, http://www.fatf-gafi.org/pages/faq/moneylaundering (last visited Jan. 24, 2014); *see also The IMF and the Fight Against Money Laundering and the Financing of Terrorism*, IMF (Sept. 30, 2013), http://www.imf.org/external/np/exr/facts/aml.htm.

41 Peter Reuter & Edwin M. Truman, CHASING DIRTY MONEY: THE FIGHT AGAINST MONEY LAUNDERING 3 (2004).

42 *Id.* at 25.

43 *Id.* at 3.

44 *Id.* at 30-31.

45 *Id.* at 3, 25.

in the fight against financing terrorism through money laundering.[46] These nonconventional banking systems, in which money is transferred using a network of intermediaries, pose a real danger because transfers of illegitimate funds are anonymous and ubiquitous.[47] Though IVTS are used widely for legitimate transactions, they remain particularly prone to abuse.[48]

Since 9/11, the fight against financing terrorism has focused on money laundering,[49] yet many challenges remain for law enforcement. First, terrorists can launder money through a multitude of channels, including currency exchanges, stockbrokers, casinos, automobile dealerships, insurance trading companies, gems and precious metals, Internet banking, trusts, wire transfers, ATMs, mortgages, and brokerage accounts.[50] Needless to say, the sheer variety of methods to launder money complicates the efforts of law enforcement.

Second, laundering techniques are complex and well financed. Traffickers constantly employ the latest technologies to keep "one step ahead of law enforcement" efforts.[51] And third, the laws of various nations lack the consistency needed to stop money laundering. Although most nations have enacted anti–money laundering laws, some are stronger than others.[52] As a result, money launderers conduct business in the countries with the weakest laws.[53] Indeed, the international money laundering effort "is only as strong as its weakest link."[54]

---

46 *See* Walter Perkel, *Money Laundering and Terrorism: Informal Value Transfer Systems*, 41 AM. CRIM. L. REV. 183, 183-85 (2004) (describing the three major worldwide IVTS and their use in financing terrorism); Tad Edward Thompson, *The War on Terror(ist Financing)*, 14 N.C. BANKING INST. 101, 103-04 (2010).

47 Advisory, Fin. Crimes Enforcement Network, Dep't of the Treas., Informal Value Transfer Systems (Sept. 1, 2010), *available at* http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2010-A011.pdf.

48 *See* Perkel, *supra* note 46, at 183-85 (noting that though "the vast majority of money transferred via the IVTS is clean money," they are also used extensively to finance terrorism and "[o]ther transnational criminal activity"); Thompson, *supra* note 46, at 103-04 (highlighting the enforcement challenges posed by IVTS, given their utility for both legitimate and nefarious purposes).

49 Jackie Johnson, *11th September, 2001: Will It Make a Difference to the Global Anti–Money Laundering Movement?*, J. MONEY LAUNDERING CONTROL, Summer 2002, at 9, 10-11 (detailing U.S. efforts to combat money laundering in the immediate aftermath of 9/11).

50 *See* 2 BUREAU FOR INT'L NARCOTICS AND LAW ENFORCEMENT AFFAIRS (INL), U.S. DEP'T OF STATE, *Money Laundering and Financial Crimes* XII-1, XII-4 [hereinafter 2 INL, *Money Laundering and Financial Crimes*], *available at* http://www.state.gov/documents/organization/8703.pdf, *in* INTERNATIONAL NARCOTICS CONTROL STRATEGY REPORT (2002); Bruce Zagaris & Scott Ehlers, *Drug Trafficking & Money Laundering*, FOREIGN POL'Y IN FOCUS (Oct. 6, 2005), http://fpif.org/drug_trafficking_money_laundering (describing the third stage of money laundering in which "a legitimate explanation for the fund is created").

51 Bachus, *supra* note 39, at 846.

52 *Id.*

53 *Id.* at 846-47; *see also* INL, *Money Laundering and Financial Crimes* 34-55, *available at* http://www.state.gov/documents/organization/204280.pdf (discussing "Major Money Laundering Countries" and listing "Jurisdictions of Primary Concern" that are particularly vulnerable to

2. Charities and Trusts

Though terrorists frequently launder money through financial markets and other expected channels, terrorism is also heavily financed through legitimate means, such as charities and trusts.[55] Because of the generally unregulated nature of these funds, terrorists' exploitation of charitable and nonprofit resources presents one of the most "serious challenges" for law enforcement.[56] Terrorist organizations often exploit the principle of *zakat*, or charity—one of the five pillars of Islam.[57] Charities elicit funding from a variety of sources, including "membership subscriptions, donations, sales of publications, . . . and appeals to wealthy members of the community."[58]

Another challenge for law enforcement—particularly in the United States—is that the freedoms of speech, association, and religion may stymie government intervention to stop the funding of terrorism through charitable and nonprofit foundations.[59] Terrorist groups have enjoyed particular success since the Cold War, funding their operations through such organizations by appealing to religious and social commonalities.[60] They have

money laundering "because of weak or nonexistent supervisory or enforcement regimes or weak political will"), *in* INTERNATIONAL NARCOTICS CONTROL STRATEGY REPORT (2013).

54 FATF, GLOBAL MONEY LAUNDERING & TERRORIST FINANCING THREAT ASSESSMENT 50 (2010), *available at* http://www.fatf-gafi.org/media/fatf/documents/reports/Global%20Threat%20assessment.pdf.

55 *See* Anna Gardella, *The Fight Against the Financing of Terrorism Between Judicial and Regulatory Regulation*, 6 STUD. INT'L FIN. ECON. & TECH. L. 109, 111 (2003); *see also* Daryl Shetterly, Note, *Starving the Terrorists of Funding: How the United States Treasury is Fighting the War on Terror*, 18 REGENT U. L. REV. 327, 329 (2006) ("[U]nlike money laundering, terrorist financing often originates with legitimate organizations and travels through customary channels. While money laundering 'depends on the existence of an underlying crime, terrorist financing does not.' It is often difficult, if not impossible, to determine whether funds are destined for a terrorist organization until they are actually delivered." (footnote omitted)).

56 Gardella, *supra* note 55, at 115-16; *see also* Bruce Zagaris, *The Merging of the Counter-Terrorism and Anti–Money Laundering Regimes*, 34 LAW & POL'Y INT'L BUS. 45, 51-52 (2002) (providing examples of charities with ties to the Middle East and Central Asia used to fund al-Qaeda).

57 Ilias Bantekas, *The International Law of Terrorist Financing*, 97 AM. J. INT'L L. 315, 322 (2003) ("The source of *zakat* is the Qur'an itself, the primary source of legal and religious reference in Islamic law. The Qur'an sets out five lawful recipients of *zakat*. Of particular interest are those described as *sabil Allah*, which refers to persons engaging in deeds for the common good of a particular Muslim society. Terrorist groups have construed *sabil Allah* to encompass violence against non-Muslim Western targets.").

58 Gardella, *supra* note 55, at 114.

59 *See* Kathryn A. Ruff, Note, *Scared to Donate: An Examination of the Effects of Designating Muslim Charities as Terrorist Organizations on the First Amendment Rights of Muslim Donors*, 9 N.Y.U. J. LEGIS. & PUB. POL'Y 447, 477-82 (2005) (explaining the effect of First Amendment freedoms on combating terrorism).

60 Bantekas, *supra* note 57, at 321-22.

infiltrated established charities to hide their funding.[61] Such "funds have been used to recruit terrorists, fund administrative activities of the organizations and support families of killed, arrested, or injured terrorists."[62] Unfortunately, many of these charitable organizations have been unaware that their funds were being used to support terrorism.[63]

In addition to charities, terrorists move money through trusts in order to take advantage of privacy laws that conceal trust formation data.[64] For example, "blind trusts" can be set up without reference to the beneficiaries or purpose of the trust.[65] Also, some jurisdictions allow for "flee clauses," which "provide for the automatic transfer of the trust to another jurisdiction if the trust becomes the subject of any sort of enquiry."[66] The anonymity and privacy afforded by trusts are attractive qualities, since the true or "beneficial" owners, as well as the recipients of the funds (including terrorist organizations), can be hidden beneath layers of corporate identities.[67] The U.N. Security Council has implicated Islamic trusts in a variety of terrorist acts, including the 2008 bombings in India and arms dealing in Afghanistan.[68]

---

61 *See* Victor Comras, *Al Qaeda Finances and Funding to Affiliated Groups* (noting that since September 11, the U.N. al Qaeda and Taliban Sanctions Committee has identified about two dozen charities as shells for terrorist funding, though they are thought to be "only the tip of the iceberg"), *in* TERRORISM FINANCING AND STATE RESPONSES: A COMPARATIVE PERSPECTIVE 115, 130-32 (Jeanne K. Giraldo & Harold A. Trinkunas eds., 2007).

62 Rebecca Gregory, *The Lawyer's Role: Will Uncle Sam Want You in the Fight Against Money Laundering and Terrorism?*, 72 UMKC L. REV. 23, 45 (2003); *see also* U.K. CHARITY COMM'N, *How Might a Charity Be Abused for Terrorist Purposes?*, PROTECTING CHARITIES FROM HARM: COMPLIANCE TOOLKIT, ch. 1, module 3, at 3 (2012), *available at* http://www.charitycommission.gov.uk/media/90832/tkch1mod3.pdf (noting that charity assets can "be used to transport people, cash, weapons or terrorist propaganda").

63 *See* Anne L. Clunan, *The Fight Against Terrorist Financing*, 121 POL. SCI. Q. 569, 570 (2006) ("Charities raising funds for humanitarian relief in war-torn societies may or may not know that their funds are going to terrorism. Corrupt individuals at charities or at recipient organizations may divert funds to terrorist organizations. This appears to be one of the main means through which al Qaeda raises funds.").

64 *See* Bantekas, *supra* note 57, at 323 (noting that in most jurisdictions, "strict privacy rules . . . help conceal the identity of the various parties . . . behind the trust," and noting further that trusts "can evidently be used by terrorists to launder illegal money and also to circulate funds without danger of being detected by channeling them through financial institutions").

65 *Id.*

66 FATF, REPORT ON MONEY LAUNDERING TYPOLOGIES 2000–2001, at 19-20 (2001), *available at* http://www.cbr.ru/today/anti_legalisation/fatf/typ-00-01.pdf; Bantekas, *supra* note 57, at 323.

67 PUPPET MASTERS, *supra* note 17, at 20-23.

68 *See, e.g.*, *Nature of the Threat of Terrorist Abuse and Exploitation of Non-Profit Organizations (NPOs)*, U.S. DEP'T OF STATE (U.S. Embassy, Kabul, Afghanistan), 2012, *available at* http://kabul.usembassy.gov/media/doco.pdf (implicating "the charitable arm of Lashkar-e-Tayba" in the 2008 terrorist attacks in Mumbai); Press Release, U.S. Dep't of Treasury, Treasury Identifies New Aliases of Al Rashid and Al-Akhtar Trusts Pakistan-Based Trusts Previously Designated for Supporting al Qaida (Jul. 2, 2008), *available at* http://www.treasury.gov/press-center/

3. Shell Companies

Finally, terrorists use shell companies to conceal and transfer money through bank accounts around the globe, including transfers within the United States.[69] Like trusts, shell companies possess an important quality: identity protection.[70] They obscure true beneficial ownership to the detriment of law enforcement worldwide.[71] In fact, as the United States has pushed heavily to prevent money laundering and illegal money transfers, the use of shell companies has increased.[72]

A shell company is a business entity with no significant assets or ongoing business activities, which is capable of transferring large sums of money worldwide.[73] "Shell companies . . . typically have no physical presence other than a mailing address, employ no one, and produce little to no independent economic value."[74] They are also easily formed, and many states do not require ownership disclosure.[75] They are often formed "to conduct legitimate transactions, such as domestic and cross-border currency and asset transfers, or to facilitate corporate mergers and reorganizations."[76]

---

press-releases/Pages/hp1065.aspx (identifying aliases of trusts "associated with Usama bin Laden, al Qaida or the Taliban").

69 *See* PUPPET MASTERS, *supra* note 17, at 37 (explaining how shell companies "[c]onceal [o]wnership of [b]ank [a]ccounts").

70 *See* Verret, *supra* note 17, at 890-92 (noting the difficulty of assessing the identity of the owner of a shell company).

71 *See* PUPPET MASTERS, *supra* note 17, at 35-36 (noting that shell companies' lack of "economic activity" can "make[] it difficult to find out much information about them"); Comras, *supra* note 61, at 124 (explaining the difficulty of regulating shell companies when they "protect [al Qaeda's financial facilitators'] identity and the identity of other financial contributors"); Chizu Nakajima, *Politics: Offshore Centres, Transparency and Integrity: The Case of the UK Territories* ("The lack of an official registry or strict banking secrecy laws makes identification of the beneficial owners of legal entities very difficult."), *in* GLOBAL FINANCIAL CRIME: TERRORISM, MONEY LAUNDERING, AND OFFSHORE CENTRES 219, 239 (Donato Masciandaro ed., 2004); Verret, *supra* note 17, at 891 ("Law enforcement personnel assert that the use of corporate shell companies hampers their ability to investigate corporate suspects.").

72 *See They Sell Sea Shells*, *supra* note 16, at 2 ("One reason for [shell companies'] ubiquity is an American-led push against money laundering. . . . [S]hell companies have become the easiest way for a malefactor to hide his identity.").

73 *See* FIN. CRIMES ENFORCEMENT NETWORK, *supra* note 16, at 2 (stating that shell companies "allow[] for the movement of billions of dollars internationally by unknown beneficial owners"); Krzysztof Woda, *The Analysis of Money Laundering Techniques* (naming shell corporations as a primary method of transferring large sums of money), *in* CYBER WARFARE AND CYBER TERRORISM 138, 141 (Lech J. Janczewski & Andrew M. Colarik eds., 2008); *see also* PUPPET MASTERS, *supra* note 17, at 34 (defining a shell company as a "non-operational company—that is, a legal entity that has no independent operations, significant assets, ongoing business activities, or employees").

74 FIN. CRIMES ENFORCEMENT NETWORK, *supra* note 16, at 4.

75 *Id.* at 2-3.

76 *Id.* at 4.

In fact, their use is vital to the operation of many businesses and to the economies of many nations. For example, shell companies in the Netherlands engage "in an estimated $1 trillion in transactions each year," and the taxes these companies pay are an important source of revenue for the government.[77]

Shell companies are so popular that an incorporation services industry has developed worldwide to cater to desiring clients. One of the most attractive characteristics of shell companies is that they protect their owners' privacy. For instance, a Wyoming business-incorporation specialist's website advertised that "[a] corporation is a legal person created by state statute that can be used as a fall guy, a servant, a good friend, or a decoy. . . . A person you control . . . yet [you] cannot be held accountable for its actions. Imagine the possibilities!"[78] Another such "incorporation agent" in London "promotes Delaware . . . as 'an offshore tax haven for non-U.S. residents'" and notes the advantages of shell companies, including that "'[o]wners' names are not disclosed to the state,' and 'the company is not required to report any assets.'"[79] Another website advertises that for under seventy dollars, it can create a corporation in Nevada that "may provide for anonymous ownership and bearer shares."[80]

In 2009, more than two million shell companies were formed in the United States alone.[81] Terrorists, in particular, view shell companies as an attractive medium to move money anonymously around the world.[82] They can be used as a "back door to the U.S. financial system," and allow terrorists—and

---

77 Gregory Crouch, *Shaken Trust: The Netherlands Rethinks an Offshore Industry*, N.Y. TIMES, Feb. 19, 2004, at C1. Shell companies are also an important source of revenue for various states within the United States, which makes identity-reporting requirements particularly unattractive to state governments. *See* Dennis Lormel, *Shell Companies . . . Facilitation Tool for Money Laundering and Terrorist Financing*, COUNTERTERRORISM BLOG (Apr. 23, 2007, 12:16 PM), http://counterterrorismblog.org/2007/04 (concluding that, before Congress can create uniform regulation of shell companies, it "must address the likely adverse impact any regulation would have on state revenues, resources and budgetary demands").

78 Kelly Carr & Brian Grow, *Special Report: A Little House of Secrets on the Great Plains*, REUTERS (June 28, 2011), http://www.reuters.com/article/2011/06/28/us-usa-shell-companies-idUSTRE75R20Z20110628 (citation omitted).

79 Elizabeth MacDonald, *Shell Games*, FORBES, Feb. 12, 2007, at 96, 99.

80 *Id.* The site also promoted "shelf" corporations, which are dormant incorporated businesses with a past operating history. *Id.*

81 Lynnley Browning, *Delaware Laws, Helpful to Arms Trafficker, to Be Scrutinized*, N.Y. TIMES (Nov. 4, 2009), http://www.nytimes.com/2009/11/05/business/05tax.html?scp=1&sq=Delaware%20Laws,%20Helpful%20to%20Arms%20Trafficker,%20to%20Be%20Scrutinized&st=cse.

82 Tom Herman, *Tax Report: IRS Cracks Down on Dodgers Who Use Onshore Tax Havens*, WALL ST. J., Dec. 6, 2006, at D2.

their financial supporters—to evade sanctions.[83] Indeed, many terrorist groups have used shell companies to launder and obscure their ties to illegal funds.[84] Terrorist organizations can further "distance themselves from the actual formation of specific shell companies by using company formation agents"[85] or by appointing puppet nominees to leadership positions of the company to allow the true owners to hide their identities.[86] Indeed, one expert opined "that of all the organisations employing money-laundering techniques, terrorist organisations are probably the most trained and adept at disguising their own origins as well as those of their funds."[87]

After the events of 9/11, however, shell companies and lax financial reporting laws faced increased scrutiny, particularly at the state level. Senator Carl Levin of Michigan, a principal proponent of reforms in this area, argued that "[w]ithin our own borders, the laws of some states regarding the formation of legal entities have significant transparency gaps which may even rival the secrecy afforded in the most attractive tax havens."[88] Due to these regulatory gaps, the Financial Crime Enforcement Network (FinCEN) received 1002 Suspicious Activity Reports between 1996 and 2005 identifying suspicious financial "activity that appear[ed] to be related to shell companies."[89] Of these reports, 768 involved suspicious international wire transfers.[90]

There is no simple mechanism, however, to detect and eliminate shell companies. State officials contend that it would be too costly to investigate all the private companies seeking to incorporate, and that disclosing the

---

83 *See* Glenn R. Simpson, *ABN Amro to Pay $80 Million Fine Over Iran, Libya*, WALL ST. J., Dec. 20, 2005, at A3 (describing the Treasury Department's critical view of shell companies, especially following 9/11).

84 *See* MacDonald, *supra* note 79, at 96 (noting how individuals associated with al-Qaeda have used shell companies in Utah and California "to commit bank fraud and money laundering and possibly to fund terrorist activities in the Middle East"); *see also* Glenn R. Simpson, *Palestinian Bank Faces U.S. Probe on Laundering*, WALL ST. J., Feb. 2, 2005, at B3 (describing a "major crackdown" on the use of shell companies to fund terrorism).

85 JEROME P. BJELOPERA & KRISTIN M. FINKLEA, CONG. RESEARCH SERV., R41547, ORGANIZED CRIME: AN EVOLVING CHALLENGE FOR U.S. LAW ENFORCEMENT 15 (2010).

86 *See* Carr & Grow, *supra* note 78 (revealing that some states "allow the real owners of corporations to hide behind 'nominee' officers and directors with no direct role in the business").

87 Martin S. Navias, *Finance Warfare as a Response to International Terrorism*, 73 POL. Q. 57, 66 (Issue Supp. s1 2002).

88 155 CONG. REC. 6922 (2009) (statement of Sen. Carl Levin).

89 FIN. CRIMES ENFORCEMENT NETWORK, *supra* note 16, at 11.

90 *Id.* Osama bin Laden used "his experience of money transfer techniques"—his "main area of technical specialisation"—to aid al-Qaeda's terrorist attacks. Navias, *supra* note 87, at 61. Saudi officials have determined that bin Laden used a network of more than fifty shell companies worldwide to launder money. Glenn R. Simpson, *Letter Suggests Saudis Supported Citizen's Censure*, WALL ST. J., Sept. 10, 2002, at A4.

names of shareholders would violate employers' privacy.[91] The fact that shell company assets often come from legitimate sources makes it difficult for law enforcement, because, in the past, most funds used to support illegal activities were obtained illicitly.[92] Terrorists' expert ability to move and conceal funds further complicates attempts at detection.[93] Although the complex nature of transactions involving shell companies makes detection difficult, some critics argue that it is not as difficult as it seems. Richard K. Gordon, a former specialist in money laundering and terrorist financing at the IMF, contends, "It's not like we're infiltrating the Mafia, where it takes five years to get insiders."[94]

Terrorist groups understand the truth of the saying that "dirty money is best passed through clean hands."[95] They abuse legal entities that can be used for legitimate purposes, such as charities, trusts, and shell companies, and the lax regulatory schemes that govern them, to evade detection by law enforcement and circulate millions of dollars around the world. Lawmakers and law enforcement officials face the challenge of balancing the interests of many legitimate users of shell companies with the need to cut off terrorists' funding.

B. *Defunding Terrorism: Domestic Efforts*

This Section describes domestic efforts to combat terrorism since September 11 across all branches of the federal government and various sectors of the U.S. economy.

---

91 *See* Marcia Coyle, *Feds Want More Corporate Data*, NAT'L L.J., Jan. 11, 2010, at 1 ("State treasurers . . . contend [that additional disclosure requirements] would federalize state incorporation practices and impose costly and onerous administrative burdens on the states and small business."). *But cf.* Zulima V. Farber & Khizar A. Sheikh, *Employers and Homeland Security: The United States' Strategy for Combating Terrorism and Its Direct Impact on Employers*, N.J. LAW. MAG., Oct. 2007, at 44, 48-49 (discussing the legislative changes regarding governmental access to information and noting that "the government has acted to assist employers . . . by issuing guidance that includes how to protect employee rights").

92 *See* Navias, *supra* note 87, at 68 (discussing the unique sources of funding for terrorist organizations that differentiate them from other criminal organizations and explaining that "where sources of funding are legal there may be few if any indicators that would identify any individual financial transaction . . . as being linked to terrorist operations").

93 *See* Douglas Farah, *Al Qaeda's Finances Ample, Say Probers*, WASH. POST, Dec. 14, 2003, at A1 ("[Terrorist financiers] are men of resources, men of high finance who know how to reformulate their businesses and how to move money.").

94 Jerry Markon, *Muslim Anger Still Burns Over Probe of Charities*, WASH. POST, Oct. 11, 2006, at B1.

95 Barbot, *supra* note 39, at 162.

1. U.S. Military, Security, and Intelligence Efforts

As described above, the United States has spent an unprecedented amount of money on its military, security, and intelligence efforts to combat terrorism.[96] Additionally, the Department of Homeland Security (DHS)[97] and its companion agencies, such as the Transportation Security Administration (TSA),[98] have brought together law enforcement and intelligence agencies to combat terrorism. DHS's broad mandate is, in part, to "(A) prevent terrorist attacks within the United States; (B) reduce the vulnerability of the United States to terrorism; [and] (C) minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States."[99]

The United States' efforts also reached outside the country, and the Department of Defense (DOD) and the Department of Justice (DOJ) quickly evolved to deal with both emerging domestic and international threats. Specifically, the DOD shifted its focus to preventing acts of terror and increased its domestic involvement in the incapacitation of potential terrorists.[100] Additionally, instead of taking military action only "against state sponsors of terrorism," the DOD exercised military force in countries

---

96 *See supra* notes 30-34 and accompanying text.

97 The DHS was organized merely eleven days after the September 11 attacks, with former Pennsylvania Governor Tom Ridge as its first director. *Creation of the Department of Homeland Security*, DEP'T OF HOMELAND SECURITY, http://www.dhs.gov/creation-department-homeland-security (last visited Jan. 24, 2014). It brought together more than twenty-two government organizations that were responsible for different aspects of security in the United States. *Id.*; *see also* PRESIDENT GEORGE W. BUSH, THE DEPARTMENT OF HOMELAND SECURITY 1 (2002), *available at* http://www.dhs.gov/xlibrary/assets/book.pdf (advocating for the creation of the DHS by noting that more than 100 agencies shared security responsibilities).

98 DHS now controls a host of functions within subagencies, including TSA, which was created in the immediate aftermath of 9/11 to oversee all transportation-related security activities, with a particular focus on airport security. *See* Aviation and Transportation Security Act, 49 U.S.C. § 114 (2006 & Supp. V 2012) (creating the TSA and specifying its duties and powers).

99 6 U.S.C. § 111(b)(1) (2012). With this broad-reaching authority, many fear that the DHS wields too much power. *See, e.g.*, Jonathan Thessin, *Department of Homeland Security*, 40 HARV. J. ON LEGIS. 513, 525 (2003) ("Narrowing DHS's focus to prevention—through border security, information analysis, and infrastructure protection—would improve homeland security without compromising essential emergency tasks."); Paul C. Light & James M. Lindsay, Op-Ed., *Homeland Security: Calibrating Calamity*, WASH. TIMES, July 25, 2002, at A19 ("Military force and diplomacy both contribute to national security, yet no one argues for placing them in the same agency."). Many were particularly concerned that the President was given full appointment power over five of the twenty-seven upper-level DHS officials. *See* Thessin, *supra*, at 529-30 (describing criticisms that the Homeland Security Act's appointment provisions "impinge[] upon congressional prerogatives").

100 *See* Robert M. Chesney, *The Sleeper Scenario: Terrorism-Support Laws and the Demands of Prevention*, 42 HARV. J. ON LEGIS. 1, 21-24 (2005) (arguing that the DOD played a limited, traditional military role in counter-terrorism efforts before 9/11, but it has played a preventative and increasingly domestic role since).

that harbored terrorists within their borders.[101] The DOD has also detained and interrogated terrorists within the United States—a practice that has been particularly controversial and has caused "institutional competition" between the DOD and the DOJ.[102]

The DOJ similarly expanded its authority by relying on the "federal material witness statute"[103] to detain suspected terrorists who could not otherwise be held.[104] The DOJ also detained individuals based on a statute that criminalizes the provision of any "material support" to terrorists.[105] These material support statutes quickly formed the foundation of the U.S. government's war on terror and provided the "weapon of choice" for prosecuting terrorism domestically.[106] These statutes have become central to the United States' efforts to obstruct terrorist financing.

Lawmakers also strengthened the ability of U.S. intelligence agencies to gather intelligence both domestically and internationally. Three important

---

101 *See id.* at 22-23 (explaining how the U.S. military departed from its traditional role of "act[ing] against state sponsors of terrorism" by, for example, detaining "an indeterminate number of suspected terrorists" outside of traditionally defined combat zones).

102 *Id.* at 25. Military involvement in the detention of people within the United States has been controversial. One noteworthy case involved Jose Padilla, a detainee who was an American citizen. *See id.* Although many thought that *Padilla*, which reached the Supreme Court twice, would resolve the major issues related to the military detention of potential terrorists within U.S. borders, the Supreme Court did not address those questions. *See* Padilla v. Hanft, 547 U.S. 1062, 1063 (2006) (deciding to withhold judgment on the substantive detention issues until "the necessity arises"); Chesney *supra* note 100, at 25.

103 18 U.S.C. § 3144 (2006).

104 *See* Ricardo J. Bascuas, *The Unconstitutionality of "Hold Until Cleared": Reexamining Material Witness Detentions in the Wake of the September 11th Dragnet*, 58 VAND. L. REV. 677, 682-83 (2005) (describing how the material witness statute allowed the DOJ to detain individuals who had not violated the law but were "needed as a witness in some criminal proceeding"). After 9/11, the DOJ was determined to use "every available law enforcement tool" to prevent another terrorist attack. *Id.* at 682. Previously unenforced immigration violations became the justification for numerous arrests. *Id.* To detain American citizens, the DOJ began to rely on the federal material witness statute. *Id.*; *see also* 18 U.S.C. § 3144; Viet D. Dinh, Foreword, *Freedom and Security After September 11*, 25 HARV. J.L. & PUB. POL'Y 399, 401-02 (2002) (describing the DOJ's use of material witness warrants to prevent terrorist attacks by incapacitating potential terrorists through detention).

105 18 U.S.C. §§ 2339A–2339B (2006 & Supp. V 2012). 18 U.S.C. § 2339C (2006) is also a material support statute, but it is rarely used. These provisions were originally passed in 1996, though they were seldom used until after 9/11. *See* Chesney, *supra* note 100, at 18-19 ("[N]otwithstanding the effort it took to establish [18 U.S.C. §§ 2339A–2339B], these powers resulted in very few prosecutions prior to 9/11. Section 2339A may have been used on as few as two occasions . . . one of which involved a domestic militia rather than a foreign terrorist organization. Meanwhile, § 2339B was used on only four occasions . . . ." (footnotes omitted)); *see also* Andrew Peterson, *Addressing Tomorrow's Terrorists*, 2 J. NAT'L SEC. L. & POL'Y 297, 298 (2008) (criticizing Congress for failing to "facilitate[e] the prosecution of major terrorists in civilian courts by enacting major legislative change," instead "tak[ing only] incremental steps, . . . buil[ding] on the material support-based system that it put in place in the mid-1990's").

106 Peterson, *supra* note 105, at 300-01.

developments made this happen: (1) Congress passed the PATRIOT Act to amend the Foreign Intelligence Surveillance Act of 1978 (FISA),[107] (2) the National Security Agency (NSA) implemented the "Terrorist Surveillance Program,"[108] and (3) Congress enacted the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA).[109] As a result of each of these efforts, intelligence officials can more easily prevent communication between terrorists,[110] gather intelligence domestically and internationally,[111] and centralize recommendations and directives to the President and his advisors.[112]

---

107 *See, e.g.*, 50 U.S.C. §§ 1806(k)(1), 1825(k)(1) (2006 & Supp. V 2012) (amending FISA to allow federal officers conducting surveillance for foreign intelligence information to consult and coordinate with federal law enforcement officers); *id.* § 1842(a)(1), (c)(2) (2006) (amending FISA to allow the use of "pen registers" and "tap and trace devices" against U.S. citizens and lawful permanent residents); *id.* § 1861(a)(1) (2011) (expanding the FBI's ability to apply for an order for production of "tangible things" in investigations); Viet D. Dinh & Wendy J. Keefer, *FISA and the PATRIOT Act: A Look Back and a Look Forward*, 35 GEO. L.J. ANN. REV. CRIM. PROC. iii, xviii (2006) (citing 50 U.S.C. § 1805(c)(2)(B) (2006) (repealed 2008), which allowed for surveillance of a person in varying areas and using different communications facilities on one order rather than requiring separate orders for each facility); *id.* at xvii-xviii ("Prior to September 11th, our foreign intelligence and law enforcement officers did not always have access to the most recent technology. Existing law had been drafted in a world where communications focused on land-line telephones . . . . Several provisions of the PATRIOT Act seek to bring the law up to date with current technology.").

108 *See* David E. Sanger & John O'Neil, *White House Begins New Effort to Defend Surveillance Program*, N.Y. TIMES (Jan. 23, 2006), http://www.nytimes.com/2006/01/23/politics/23cnd-wiretap.html?_r=1 (discussing President Bush's announcement and defense of the NSA's "warrantless eavesdropping program, calling it a 'terrorist surveillance program' that had saved lives"). This program drew heavy criticism. *See, e.g.*, Katherine Wong, *The NSA Terrorist Surveillance Program*, 43 HARV. J. ON LEGIS. 517, 528-34 (2006) (arguing that the terrorist surveillance program represents an unconstitutional expansion of executive power); David Cole et al., *On NSA Spying: A Letter to Congress*, N.Y. REV. BOOKS, Feb. 9, 2006, at 42, 42 (arguing that the terrorist surveillance program is illegal under existing law). In response, U.S. Attorney General Alberto R. Gonzales sent a letter to the Senate Judiciary Committee stating that "any electronic surveillance that was occurring as part of the Terrorist Surveillance Program will now be conducted subject to the approval of the Foreign Intelligence Surveillance Court." Letter from Alberto R. Gonzales, Att'y Gen., to Chairman Patrick Leahy and Sen. Arlen Specter, S. Judiciary Comm. (Jan. 17, 2007), *available at* http://graphics8.nytimes.com/packages/pdf/politics/20060117gonzales_Letter.pdf.

109 *See* 150 CONG. REC. 25,942 (2004) (statement of Sen. Tom Udall) (discussing the anticipated impact of the IRTPA); *Id.* at 19,412 (statement of Sen. Susan Collins) (referring to the IRTPA as "the most sweeping reform of our intelligence structures in more than 50 years"). The IRTPA was passed in response to the 9/11 Commission's findings regarding obstacles that might keep the United States from preventing future terrorist attacks. *See* 9/11 COMMISSION REPORT, *supra* note 2, at 339-48 (discussing the failures of U.S. counterterrorism efforts and identifying four major areas for improvement: "imagination, policy, capabilities, and management").

110 *See* U.S. DEP'T OF JUSTICE, REPORT FROM THE FIELD: THE USA PATRIOT ACT AT WORK 18-28 (2004), *available at* http://www.justice.gov/olp/pdf/patriot_report_from_the_field0704.pdf (outlining ways the PATRIOT Act has improved the United States' ability to intercept terrorist communications); Benjamin R. Davis, *Ending the Cyber Jihad: Combating Terrorist Exploitation of the Internet with the Rule of Law and Improved Tools for Cyber Governance*, 15 COMMLAW CONSPECTUS 119, 150-55 (2006) (discussing changes to the government's power, as a result of the PATRIOT Act

2. U.S. Financial Efforts

The United States has also taken significant financial measures to combat terrorism, although these actions are not as extensive as its military, security, and intelligence measures discussed above. In fact, the United States has come under heavy criticism for its lax regulatory scheme, numerous shell companies, and noncompliance with accepted international identity requirements.[113] Senator Carl Levin has noted that shell companies are required to provide "less information to the State than is required to open a bank account or obtain a driver's license."[114]

This is not to say that the United States has not taken any efforts to prevent terrorism financing. For example, pursuant to an executive order, the Department of the Treasury deprives charities and trusts access to illicit funds by giving them "terrorist designations."[115] Further, to restrict the use of shell companies for terrorist financing, the United States has occasionally enforced the material support statutes.[116] It has also worked to identify

---

and the Homeland Security Act, to combat terrorists' ability to use the internet to communicate and gain resources).

111 Under FISA, the government is now only required to show that foreign intelligence is a "significant purpose" of surveillance, amending the previous requirement that such intelligence be "the purpose." *In re* Sealed Case, 310 F.3d 717, 728-29 (FISA Ct. Rev. 2002) (discussing Congress's amendment of 50 U.S.C. § 1804(a)(7)(B) (2006)); *see also* Dinh & Keefer, *supra* note 107, at xiv-xvii (discussing how changing to the "significant purpose" test was not meant "wholly to tear down the division between law enforcement and foreign intelligence activities . . . [but to] open certain doors to prevent isolation both of investigators and the information they collect"). *See generally* John J. Dvorske, Annotation, *Validity, Construction, and Application of Foreign Intelligence Surveillance Act of 1978 (50 U.S.C.A. §§ 1801 et seq.) Authorizing Electronic Surveillance of Foreign Powers and Their Agents*, 190 A.L.R. Fed. 385 (2003).

112 *See, e.g.*, Conference Report on Intelligence Reform and Terrorism Prevention Act of 2004, 150 CONG. REC. 25,950 (statement of Rep. Eleanor Holmes Norton) ("[Before 9/11, v]arious intelligence agencies each had parts of vital information about the imminence of an attack, but they rarely communicated and never collaborated."); U.S. DEP'T OF JUSTICE, *supra* note 110, at 2-9 (describing how the PATRIOT Act allowed agencies to share information and "connect the dots").

113 *See* FATF, THIRD MUTUAL EVALUATION REPORT ON ANTI–MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM 299-303 tbl.1 (June 23, 2006) (evaluating the United States' compliance with FATF recommendations); *cf., e.g.*, Carr & Grow, *supra* note 78 (showcasing Wyoming companies that offer incorporation services).

114 155 CONG. REC. 6921 (2009) (statement of Sen. Carl Levin).

115 *See generally* U.S. DEP'T OF THE TREASURY: PROTECTING CHARITABLE GIVING (June 4, 2010), *available at* http://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/Treasury%20Charity%20FAQs%206-4-2010%20FINAL.pdf.

116 *See supra* notes 105-06 and accompanying text. To prosecute under these statutes, the government must show that a "person has knowingly provided, attempted to provide, or conspired to provide a foreign terrorist organization with 1 or more individuals (who may be or include himself) to work under that terrorist organization's direction or control or to organize, manage, supervise, or otherwise direct the operation of that organization." 18 U.S.C. § 2339B(h) (2006).

"foreign terrorist organizations" (FTOs) and block their funding domestically and abroad.[117]

The United States has made significant efforts to restrict certain transactions and regulate money laundering generally through the PATRIOT Act and the Money Laundering Control Act (MLCA).[118] The PATRIOT Act, for instance, requires that broker–dealers file Suspicious Activity Reports (SARs) and that they take extra precautions when dealing with shell companies.[119] Many of the PATRIOT Act's reforms were accomplished by amending the Bank Secrecy Act.[120] Financial institutions are also required

---

For an overview of the requirements of the material support statutes, see generally Randolph N. Jonakait, *A Double Due Process Denial: The Crime of Providing Material Support or Resources to Designated Foreign Terrorist Organizations*, 48 N.Y.L. SCH. L. REV. 125 (2003). For a critique of their use, see Peterson, *supra* note 105, at 349-53. *See also* Jeff Breinholt, *Resolved, or Is It? The First Amendment and Giving Money to Terrorists*, 57 AM. U. L. REV. 1273, 1278-81 (2008) (discussing the role First Amendment protection plays in terrorist financing laws); Chesney, *supra* note 100, at 52-55 (explaining First Amendment objections to anti–money laundering regulation).

117 Section 216 of the Immigration and Nationality Act authorizes the Secretary of State to designate a group as an FTO if three findings are made: (1) that the group is a "foreign organization;" (2) that the group "engages in terrorist activity . . . or terrorism . . . or retains the capability and intent" to do so; and (3) that the group's "terrorist activity or terrorism . . . threatens the security of United States nationals or the national security of the United States." 8 U.S.C. § 1189 (2012); *see also* 18 U.S.C. § 2339B (2006) ("[T]he term 'terrorist organization' means an organization designated as a terrorist organization under section 219 of the Immigration and Nationality Act."). The President can also influence the designation of groups as terrorist organizations under certain circumstances as detailed in IEEPA. *See* Chesney, *supra* note 100, at 18-21 (noting the increased use of IEEPA powers since 9/11).

118 *See* Alan E. Sorcher, *Lost in Implementation: Financial Institutions Face Challenges Complying With Anti–Money Laundering Laws*, 18 TRANSNAT'L LAW. 395, 396, 397 n.4 (2005) (mentioning the U.S. government's increased powers to combat money laundering and terrorist financing under the PATRIOT Act, and noting that money laundering was first recognized as a crime in its own right by the Money Laundering Control Act of 1986, 18 U.S.C. §§ 1956–1957 (2006 & Supp. V 2012)). For further details about the PATRIOT Act and its implementation, see Bruce Zagaris, *supra* note 56, at 56-68.

119 Sorcher, *supra* note 118, at 399-400, 402-03. SARs must be filed when a transaction

> is conducted or attempted by, at, or through the broker–dealer, and the broker–dealer knows, suspects, or has reason to suspect that the transaction (or a pattern of transactions): (1) involves funds derived from illegal activity, or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity; (2) is designed, whether through structuring or other means, to evade the requirements of the Bank Secrecy Act; (3) has no business or apparent lawful purpose, or is not the sort in which the particular customer would be expected to engage, and the broker–dealer knows of no reasonable explanation after examining the available facts; or (4) uses the broker–dealer to facilitate criminal activity.

Id. (citing Financial Crimes Enforcement Network (FinCEN), 66 Fed. Reg. 67,670 (codified as amended at 31 C.F.R. § 103.18 (2001))).

120 Enacted by Congress in 1970, and amended multiple times, the Bank Secrecy Act (BSA)

to do more to verify the identity of their customers through "Customer Identification Programs" (CIPs), due diligence, and cross-border information sharing.[121] The PATRIOT Act also better regulates IVTS,[122] which, as discussed above, are utilized heavily in the Middle East and Asia to launder money through currency exchanges.[123] The United States has also relied on the MLCA, enacted in 1998, to enforce reporting requirements and to regulate foreign money laundering through U.S. banking institutions.[124]

> is based on the assumption that it is easiest for law enforcement to detect and prosecute money laundering during the placement phase of the process, since the money is closest to its origin at that point in time, and the financial institutions used for placement can be regulated through mandatory reporting requirements.

Kathleen A. Lacey & Barbara Crutchfield George, *Crackdown on Money Laundering: A Comparative Analysis of the Feasibility and Effectiveness of Domestic and Multilateral Policy Reforms*, 23 NW. J. INT'L L. & BUS. 263, 294-95 (2003) (citing Barbot, *supra* note 39). One of the BSA's more relevant provisions requires domestic banking institutions to file a Currency Transaction Report (CTR) if "$10,000 or more is withdrawn or deposited into one account in a single day." *Id.* at 295-96 (citing transaction reporting requirements found in 31 U.S.C. § 5313 (2000 & Supp. II 2002) requiring "a domestic financial institution . . . involved in a transaction for the payment, receipt, or transfer of United States coins or currency . . . in an amount, denomination, or amount and denomination, or under circumstances the Secretary prescribes by regulation . . . [to] file a report on the transaction"). CTRs also "must disclose the identity of the customer who has the account and the customer's source of funds." *Id.* at 296. Additionally, banks are not allowed to inform any person involved in a suspicious transaction that the transaction has been reported to the government. *Id.* (citing 31 U.S.C. § 5318(g)(2) (2000 & Supp. II 2002)).

121 Sorcher, *supra* note 118, at 400-04. CIPs specifically require that

> [f]irms . . . obtain the following information [from each customer] prior to opening an account: (1) name; (2) date of birth (for individuals); (3) residential or business street address for individuals, or principal place of business, local office or other physical location for persons other than individuals; and (4) identification number—for a U.S. person, a taxpayer identification number ("TIN"); for a non-U.S. person, a TIN, a passport number and country of issuance, an alien identification card number or the number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.

Id. at 400-01.

122 31 U.S.C. § 5312(a)(2)(R) (2006) (including in the definition of "financial institution . . . any . . . person who engages as a business in an informal money transfer system or any network of people who engage as a business in facilitating the transfer of money domestically or internationally outside of the conventional financial institutions system"); Shetterly, *supra* note 55, at 344-45 (describing the Treasury Department's new IVTS-related authority). This enhanced regulation is significant because it is estimated that billions of dollars annually cross many of the Arab nations' and Pakistan's borders through *hawala*, which are IVTS "preferred by Arabs[,] . . . from the Arabic word meaning trust." *See id.* ("Congress and the Treasury have made *hawala* a priority since the attacks of September 11, 2001, and the discovery that *hawala* were used to fund at least two of the highjackers: Mohammad Atta and Marwan al-Shehhi.").

123 *See supra* notes 46-48 and accompanying text.

124 *See* 18 U.S.C. §§ 1956–1957 (2006 & Supp. V 2012) (prohibiting money laundering and "[e]ngaging in monetary transactions in property derived from specified unlawful activity").

More recently, Senator Levin has pushed to enact the Incorporation Transparency and Law Enforcement Assistance Act (ITLEA), which would expose the beneficial owners of shell companies.[125] Previous versions of the ITLEA have enjoyed support from both political parties[126] as well as various policy and business groups,[127] but the Act has also faced significant criticism for its reliance on voluntary reporting and lack of significant incentives or penalties for nonreporting.[128] For example, it conditions state antiterrorism funding on an additional identity reporting requirement, but it does not penalize states for declining "to verify the information."[129] Because of loopholes in the current regulatory framework, U.S. firms and incorporation services are required to collect only minimal identity information. Surprisingly, *international* identity reporting requirements are more stringent and have been adopted almost universally, as discussed below.

C. *Defunding Terrorism: International Efforts*

The fight against terrorist financing requires international collaboration not only among nations but also internally among government agencies and private firms.[130] Although the United States has fallen short with its own internal efforts in many respects, there has been a significant international push to stop terrorism financing through money laundering, charities, trusts, and anonymous shell companies. Foremost among those efforts has

"Under the [MLCA], it is unlawful to intentionally promote . . . [the] avoidance of reporting requirements, usually referred to as 'smurfing.'" Barbot, *supra* note 39, at 186 (footnote omitted). This refers to making "a deposit in an amount slightly less than $10,000" in order to avoid a CTR being filed. *Id.* at n.116 (citing Duncan E. Alford, *Anti–Money Laundering Regulations: A Burden on Financial Institutions*, 19 N.C. J. INT'L L. & COM. REG. 427, 458 (1994)). The MLCA also requires the U.S. Treasury Department to file annual reports detailing its efforts. *Id.*

125 S. 1465, 113th Cong. (2013); *see also* Carr & Grow, *supra* note 78 ("Senator Carl Levin[,] . . . chairman of the Senate Homeland Security Committee's Permanent Subcommittee for Investigations, has introduced the [ITLEA] each year since 2008.").

126 *E.g.*, Press Release, Global Fin. Integrity, Incorporation Transparency and Law Enforcement Assistance Act Introduced Today (Aug. 2, 2011), *available at* http://www.financialtaskforce.org/2011/08/02/incorporation-transparency-and-federal-law-enforcement-act-introduced-today.

127 *E.g.*, EJ Fagan, *Why We Need the Incorporation and Law Enforcement Assistance Act*, FIN. TRANSPARENCY COALITION (May 16, 2012), *available at* http://www.financialtaskforce.org/2012/05/16/why-we-need-the-incorporation-transparency-and-law-enforcement-assistance-act; Press Release, Fin. Accountability and Corp. Transparency (FACT) Coal., Civil Society, Business Groups Call on Congress to Support Incorporation Transparency, Ban Anonymous U.S. Shell Companies (May 16, 2012), *available at* http://www.financialtaskforce.org/2012/05/16/civil-society-business-groups-call-on-congress-to-support-incorporation-transparency-ban-anonymous-u-s-shell-companies.

128 *See generally* Verret, *supra* note 17.

129 *See* 157 CONG. REC. S5255 (daily ed. Aug. 2, 2011) (statement of Sen. Carl Levin).

130 Success essentially requires "re-conceptualizing the public good of open financial systems as having negative security externalities that must be collectively managed." Clunan, *supra* note 63, at 571.

been the creation of, and the issuance of recommendations by, the FATF—an intergovernmental organization working to combat money laundering and terrorism financing.[131] The FATF was established during the 1989 G-7 Summit in Paris and has grown to include thirty-six member countries, each of which provides experts to serve on the body's governing panel.[132]

Though its recommendations are not legally binding on its members, the FATF does require member self-assessments and "blacklist[s]" countries it deems "non-cooperative," for such reasons as "obstacles within a jurisdiction's financial regulatory regime[,] . . . inadequate or lack of resources devoted to anti–money laundering efforts, and obstacles to international cooperation."[133] In addition, FATF-compliant countries threaten countermeasures against money from "non-cooperative countries or territories" that "d[o] not correct identified problems within one year."[134]

The United Nations has also taken steps to curb terrorism financing and money laundering. For example, the U.N. Security Council (UNSC) has given terrorist designations to Pakistani trusts that have provided financial support to terrorists and supported bombing attacks in India.[135] In fact, in 1999—prior to the 9/11 attacks—the U.N. General Assembly adopted the International Convention for the Suppression of the Financing of Terrorism.[136] This convention "criminalize[s] the collection or provision of funds with the knowledge or intent that they be used to conduct certain terrorist activity," implements many of the FATF's Forty Recommendations on Money Laundering, and encourages financial institutions to report suspicious transactions.[137] A mere seventeen days after 9/11, the UNSC also adopted Resolution 1373[138]—a true centerpiece in the international effort to fight

131 Sorcher, *supra* note 118, at 405-08.

132 *Id.* at 405-06; *see also FATF Members and Observers*, FATF, http://www.fatf-gafi.org/pages/aboutus/membersandobservers (last visited Jan. 24, 2014).

133 Bachus, *supra* note 39, at 851-53; *see also High-Risk and Non-Cooperative Jurisdictions*, FATF, http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/documents/fatf-compliance-oct-2013.html (last updated Oct. 18, 2013).

134 Bachus, *supra* note 39, at 852-53.

135 *See supra* note 68 and accompanying text.

136 International Convention for the Suppression of the Financing of Terrorism, G.A. Res. 54/109, U.N. GAOR, 54th Sess., Supp. No. 49 (Vol. 1), at 408, U.N. Doc. A/54/49 (Dec. 9, 1999), *entered into force* Apr. 10, 2002.

137 Sorcher, *supra* note 118, at 411.

138 *See* Zagaris, *supra* note 56, at 75-76 (citing S.C. Res. 1368, U.N. SCOR, 56th Sess., U.N. Doc. S/RES/1368 (Sept. 12, 2001) (requiring states to (1) prevent and suppress the nuancing of terrorist financing; (2) freeze without delay the resources of terrorist and terror organizations; (3) prohibit anyone from making funds available to terrorist organizations; (4) suppress the recruitment of new members by terrorism organizations; (5) deny safe haven to those who finance, plan, support, or commit terrorist acts, or those who provide safe havens; (6) afford one another the greatest

terrorism, both because of its requirement that states criminalize terrorism financing and its creation of an implementing committee.[139] The examples above represent just a few of the UN's numerous proactive measures to combat terrorism financing.[140]

The European Union has also made significant efforts to adopt the FATF's recommendations. One Directive, for instance, closely follows the FATF's Forty Recommendations and requires member states to identify customers, keep thorough records, and report any suspicious transactions.[141] The Directive is binding on all EU members and can be enforced through legal proceedings.[142] The Directive was replaced in 2004—in part due to 9/11—by a new Directive that "specifically covers terrorist financing and provides for more detailed customer identification and verification procedures."[143] Additionally, because the problem of terrorism financing reaches beyond the scope of the European Union's financial and banking institutions, it has imposed "gatekeeper" standards[144] on lawyers, accountants, and real estate agents.[145]

measure of assistance in criminal investigations involving terrorism; and (7) prevent the movement of terrorists or terrorist groups by effective border controls and control over travel documentation)).

139 Press Release, Security Council, Security Council Unanimously Adopts Wide-Ranging Anti-Terrorism Resolution; Calls for Suppressing Financing, Improving International Cooperation, U.N. Press Release SC/4385 (Sept. 28, 2001), *available at* www.un.org/News/Press/docs/2001/sc7158.doc.htm; *see also* S.C. Res. 1373, U.N. SCOR, 56th Sess., 4385th mtg., U.N. Doc. S/RES/1373 (Sept. 28, 2001); Gardella, *supra* note 55, at 125-28 (describing the requirements of the resolution); Zagaris, *supra* note 56, at 75-76 (same).

140 In addition to the examples described above, "[t]he UN Convention Against Transnational Organized Crime was the first legally binding multilateral treaty specifically aimed at transnational organized crime." Sorcher, *supra* note 118, at 411. Also, the "United Nations Office for Drug Control and Crime Prevention (ODCCP) provides member nations with assistance in complying with international anti–money laundering standards." Bachus, *supra* note 39, at 856 (citing 2 INL, *Money Laundering and Financial Crimes*, *supra* note 50, at XII-52). For a review of several other U.N. initiatives, see Lacey & George, *supra* note 120, at 332-35.

141 Council Directive 91/308/EEC, 1991 O.J. (L 166) 77 (E.C.).

142 Sorcher, *supra* note 118, at 408.

143 *Id.*; *see also* Council Directive 2005/60/EC, 2005 O.J. (L 309) 15 (E.C.).

144 These "gatekeeper" standards originated at the G-8 Summit and have since been endorsed by the European Union, FATF, the United States (through the PATRIOT Act), and a host of other nations. *See* Gregory, *supra* note 62, at 32-38, 46-50.

145 *Id.* at 32, 35. The American Bar Association (ABA) created its own Task Force on Gatekeeper Regulation and Profession in 2002 to monitor compliance with these standards. *Id.* at 38; *see also* ABA TASK FORCE ON GATEKEEPER REGULATION AND THE PROFESSION, COMMENTS OF THE ABA TASK FORCE ON GATEKEEPER REGULATION AND THE PROFESSION ON THE FINANCIAL ACTION TASK FORCE CONSULTATION PAPER DATED MAY 30, 2002, at 2-3 (2002), *available at* http://www.abanet.org/crimjust/taskforce/comments.doc.

D. *Remaining Domestic Challenges*

Despite the complex domestic and international framework that has emerged since 9/11, and notwithstanding the enormous sums spent by the United States and the international community on policing terrorism financing, two major enforcement gaps remain. Moreover, terrorist groups' greater access to funding through virtual channels such as the Internet exacerbates these problems.[146]

First, the United States' lax domestic policies and federalism challenges to virtual regulation facilitate the formation of anonymous shell companies.[147] Relaxed state laws in Delaware, for example, have allowed Jack Abramoff and Viktor Bout—the infamous Russian Arms dealer dubbed the "Merchant of Death"—to form anonymous shell corporations.[148] Even officials in the Cayman Islands, a country widely regarded as a tax haven, criticize that "Delaware is today playing faster and looser than the offshore jurisdictions that raise hackles in Washington."[149] "Delaware is the state that requires the least amount of information,"[150] and its approach to incorporation and LLC formation attracts companies from around the world—legitimate and otherwise.[151]

Although the federal government wishes to impose more thorough reporting requirements (seen most recently through Senator Levin's sponsorship of the ITLEA), federalism issues present another obstacle to implementation. For example, in a 2006 report, the FATF specifically noted the United States' failure to designate as offenses noncompliance with certain reporting requirements.[152] Some of this failure may stem from the anticommandeering

---

146 *See* Stephen I. Landman, *Funding Bin Laden's Avatar: A Proposal for the Regulation of Virtual* Hawalas, 35 WM. MITCHELL L. REV. 5159, 5180-83 (2009) (discussing the difficulties of regulating virtual exchanges and proposing expansions to current law to reach the virtual marketplace).

147 *See* Browning, *supra* note 81, at 1 ("Delaware and . . . other states have business-friendly laws that encourage the creation of opaque shell companies, allowing their true owners to be disguised or obscured.").

148 *Id.*; Ned Resnikoff, *How to Steal a Billion in Taxes*, MSNBC (Apr. 15, 2013), http://www.msnbc.com/all-in/how-steal-billion-in-taxes.

149 Leslie Wayne, *How Delaware Thrives as a Corporate Tax Haven*, N.Y. TIMES, June 30, 2012, at BU1.

150 *E.g.*, *id.* (quoting David Finzer, chief executive of a registration agent that sets up accounts for non-U.S. citizens).

151 *See* Verret, *supra* note 17, at 892-95 ("Delaware has designed its LLC legal regime to facilitate freedom of contract to allow parties of LLC agreements to arrange their relations according to their particular needs.").

152 FATF, *supra* note 113, at 146-47. Among its many recommendations, the report states that "[t]here remains a gap between the policy level and operational level law enforcement work," further noting that "[m]ore refined coordination is needed amongst law enforcement agencies with overlapping jurisdictions." *Id.* at 301 tbl.1. *But see* Robert Fromme & Rick Schwein, *Operation*

doctrine set forth by the Supreme Court in *Printz v. United States*, which prohibits Congress from forcing state and local governments to implement federal programs.[153] Although Congress made it clear in the PATRIOT Act that the United States' national strategy involves enhanced federal–state cooperation,[154] it often lacks the mechanisms and resources to constitutionally incentivize state compliance.[155] And there is ample evidence to suggest that states do not voluntarily comply when federal prerogatives run counter to state priorities.[156] Even the FATF noted that the United States needs more effective internal, intrastate cooperation and remarked that the current "law enforcement arena appears to be fragmented."[157] Thus, state jurisdiction over the formation of corporations and other important financial vehicles, coupled with local unwillingness to bear the costs of national antiterrorist programs, hinders a united domestic response against terrorism.

Second, the United States' current and suggested framework for fighting terrorist financing may raise business privacy and due process concerns. U.S. and international policies regarding client identity and suspicious activity reporting remain controversial, often because they could compromise

Smokescreen: A Successful Collaboration, FBI LAW ENFORCEMENT BULL., Dec. 2007, at 20, 22-24 (discussing an example of successful federal–state collaboration in fighting crime and terrorism).

153 *See* 521 U.S. 898, 921 (1997) ("This separation of the two spheres is one of the Constitution's structural protections of liberty."); Ann Althouse, *The Vigor of Anti-Commandeering Doctrine in Times of Terror*, 69 BROOK. L. REV. 1231, 1257-61 (2004) (arguing that courts should resist the temptation to dilute the anticommandeering doctrine for the sake of counterterrorism).

154 31 U.S.C. § 5341 (2006) (calling for "[t]he enhancement of[] cooperative efforts between the Federal Government and State and local officials").

155 *See* Ernest Young, *The Balance of Federalism in Unbalanced Times: Should the Supreme Court Reconsider Its Federalism Precedents in Light of the War on Terrorism?*, FINDLAW (Oct. 10, 2001), http://writ.lp.findlaw.com/scripts/printer_friendly.pl?page=/commentary/20011010_young.html (arguing in favor of robust state autonomy even during the War on Terror). Others interpret the Constitution as giving the federal government the power to force state and local governments to implement antiterrorism programs notwithstanding the anticommandeering doctrine. *See, e.g.*, Jason Mazzone, *The Security Constitution*, 53 UCLA L. REV. 29, 35-36 (2005) (noting that Article IV, Section 4 (the Protection Clause) of the Constitution requires the federal government to "*protect* the states from invasion and domestic violence"). The generation of Americans that ratified the Constitution's Protection Clause went through similar problems that "the War on Terrorism presents today: Security represents a collective-action dilemma because each state is reluctant to contribute to the costs of defending other states although the cost of an attack is not geographically confined." *Id.* at 36. Yet the Protection Clause guarantees that "the national government may enlist the assistance of state and local personnel so long as Congress pays the costs of their efforts." *Id.* at 36.

156 *See, e.g.*, Susan N. Herman, Introduction, *David G. Trager Public Policy Symposium: Our New Federalism? National Authority and Local Autonomy in the War on Terror*, 69 BROOK. L. REV. 1201, 1210 (2003–2004) (examining an instance in which local law enforcement officers refused the FBI's request for assistance, post-9/11, in questioning roughly 5000 Arabs and Muslims in Detroit and Portland).

157 FATF, *supra* note 113, at 256-58.

the attorney–client privilege.[158] However, a number of policy tools can counterbalance privacy concerns, including the use of "formal nominees" in identity reporting requirements.[159] Still, the private sector opposes these requirements, and balancing a client's privacy with combatting financial crime will most likely continue to be a difficult task. In addition, individuals and corporations who seek to transfer money anonymously criticize the current regulatory framework on First Amendment grounds.[160]

Due process is another private sector concern as assets are frozen under arguably overbroad executive powers.[161] As prosecutions are carried out under the President's executive International Emergency Economic Powers Act (IEEPA) powers, individual litigants have tried—though so far unsuccessfully—to assert due process challenges.[162] Additionally, many contend that the President's statutory authority is overbroad, since the power to make terrorist designations is sweeping and quasi-judicial.[163] These and other concerns have stalled progress as Congress attempts to strengthen the current legal and regulatory framework. What, if anything, within this framework can stop terrorism financing? Are international or domestic regulations more effective? The study that follows attempts to answer these questions by identifying which countries and institutions comply less frequently with identity reporting requirements and the factors that influence whether an institution agrees to help form a shell company.

---

158 *See id.* at 261-62 (discussing suspicious-activity reporting and the attorney–client privilege); *see also* Marc Loewenthal, *Financial Privacy Laws in Conflict*, EPOLICY (Aug. 2002), http://special.pacificresearch.org/pub/ecp/2002/epolicy08-08.html (criticizing the PATRIOT Act for requiring banks to share customer information with the government without notice to the customers).

159 PUPPET MASTERS, *supra* note 17, at 59-61.

160 *See, e.g.*, Buckley v. Valeo, 424 U.S. 1, 16 (1976) (per curiam) (striking down limits on campaign expenditures); *see also* Guiora & Field, *supra* note 38, at 62-63 (describing the problem of money laundering—particularly through IVTS—to fund terrorism, and contrasting such illegitimate uses of IVTS with legitimate charitable and religious uses).

161 *See* Aloke Chakravarty, *Feeding Humanity, Starving Terror: The Utility of Aid in a Comprehensive Antiterrorism Financing Strategy*, 32 W. NEW ENG. L. REV. 295, 309 (2010) (stating the main challenges to the statutes addressing terrorism funding).

162 *See* People's Mojahedin Org. of Iran v. U.S. Dep't of State, 182 F.3d 17, 21 (D.C. Cir. 1999) ("[T]he Secretary of the Treasury may require U.S. financial institutions that possess or control assets of that organization to block all financial transactions involving those assets . . . .").

163 *See* Global Relief Found., Inc. v. O'Neill, 315 F.3d 748, 754 (7th Cir. 2002) (refusing to enjoin the Secretary of the Treasury's order blocking corporate assets under IEEPA). For a more detailed explanation of the expansiveness of executive power in the war on terror, see Chakravarty, *supra* note 161, at 308-11.

II. EXPERIMENTAL RESULTS

While the government has done much to disrupt and dismantle terrorist networks worldwide,[164] security officials and commentators are concerned that the United States has not invested sufficient resources to cut off the true terrorist lifeline: illicit *financing*.[165] As the United States' military and intelligence efforts prove increasingly effective at dismantling terrorist networks, terrorists must seek ever more clandestine approaches to finance their activities. As described above, this has led to terrorist organizations laundering money through trusts, charities, and shell corporations.[166]

The international community has responded by developing policies to combat money laundering and terrorism financing.[167] For example, intergovernmental organizations (IGOs) and nations such as the United States have enacted extensive regulations that track FATF recommendations.[168] These efforts produced strict regulations governing the formation of shell companies. At least on paper, the "anonymous" shell corporation was completely prohibited.[169]

While these international and domestic laws have been in place for years, few empirical studies have investigated their effectiveness. Previous articles attempt to show how easy it is to form a shell company, but they have only provided anecdotal evidence or a summary of several examples.[170] By contrast, our study used 7462 approaches to 3773 providers in 181 countries. We randomly assigned a variety of approaches to determine what

---

164 *See, e.g.*, Neil H. MacBride, *No Higher Priority: Fighting Terrorism and Keeping Americans Safe*, OFF. U.S. ATT'YS, http://www.justice.gov/usao/briefing_room/ns/op-ed1.html (last visited Jan. 24, 2014) (praising the FBI's efforts in arresting "homegrown extremists" and the DOJ's efforts in prosecuting them); McNeill et al., *supra* note 33; Press Release, President Barack Obama, Remarks by the President at the National Defense University (May 23, 2013), *available at* http://www.whitehouse.gov/the-press-office/2013/05/23/remarks-president-national-defense-university (praising U.S. antiterrorism efforts since 9/11).

165 *See, e.g.*, Kern Alexander, *United States Financial Sanctions and International Terrorism* (pt. 1), 17 BUTTERWORTHS J. INT'L BANKING & FIN. L. 80, 80-88 (2002) (evaluating the multifaceted policy response to terror funding since 9/11).

166 *See supra* Section I.A.

167 *See* Chris Brummer, *How International Financial Law Works (and How It Doesn't)*, 99 GEO. L.J. 257, 295-97 (2011) (discussing the history and challenges of implementing FATF recommendations).

168 For examples of such U.S. regulations, see *supra* note 22.

169 *See generally* FATF, INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION: THE FATF RECOMMENDATIONS (2012), *available at* http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf (discussing the requirement of some form of identification to conduct certain transactions, such as a notarized passport copy and certified utility bill, to prohibit anonymous accounts or accounts in obviously fictitious names).

170 *See supra* note 24 and accompanying text.

factors cause providers to be more or less likely to comply with domestic and international regulations affecting the formation of shell companies.[171]

In our study, we attempt to answer the question of how effective the post–September 11 regulations have been at curbing the incorporation of anonymous shell corporations. We first seek to discover which countries are the most compliant and what factors might contribute to noncompliance. We then explore whether compliance in the United States differs from that elsewhere in the international community. Finally, we compare the results from both the international and domestic tests to analyze what factors make some countries more or less compliant than others.

A. *Design Study: Finding Providers, Composing Treatments*

To determine the effectiveness of post-9/11 financial regulations, we analyzed countries' informal compliance with FATF recommendations and IRS regulations by way of private actors, including firms and incorporation services providers.[172] Mindful that the field experiment is occasionally criticized for contributing only a pragmatic, "what works" analysis,[173] we focused on larger theoretical questions. Accordingly, this field experiment presents more than statistics; we utilize the major international law and relations theories to get to the heart of what actually causes compliance.[174]

To complete this experiment, we compiled a list of incorporation services providers and created a set of emails to be sent from a number of aliases through which we posed as international consultants seeking anonymous shell corporations. To find and compile the list of providers, because no definitive list exists of incorporation services providers, we performed

---

171 Full experimental results are reported in several other locations. *See* FINDLEY, NIELSON & SHARMAN, *supra* note 29; Michael G. Findley, Daniel L. Nielson & J.C. Sharman, *Using Field Experiments in International Relations: A Randomized Study of Anonymous Incorporation*, 67 INT'L ORG. 657, 673-77 (2013); Michael G. Findley, Daniel L. Nielson & J.C. Sharman, Causes of Noncompliance with International Law: A Field Experiment on Anonymous Incorporation 16-34 (Feb. 18, 2013) (unpublished manuscript) (on file with author).

172 For a more thorough analysis of formal compliance, see Shima Baradaran et al., *Does International Law Matter?*, 97 MINN. L. REV. 743, 749-51 (2013) (reporting findings from a field experiment on compliance with international financial transparency laws). Formal compliance is easier to gauge because it appears in the steps the nation takes to implement and enforce international transparency laws. *See* Brummer, *supra* note 167, at 291-92 (discussing the weaknesses that arise when international bodies attempt to monitor financial compliance). This, however, is not the focus of our study.

173 *See, e.g.*, Susan D. Hyde, *The Future of Field Experiments in International Relations*, 628 ANNALS AM. ACAD. POL. & SOC. SCI. 72, 75 (2010) (noting that field experiments are often criticized for failing to address "big questions" and only dealing with "insignificant phenomena").

174 For a discussion of managerialism and its intersection with this study, see *infra* note 201 and accompanying text.

Internet searches for terms such as "company formation" and "business law." We successfully collected a pool of 3773 corporations and law firms drawn from nearly every nation of the world—181 to be precise. Of these, 1785 were from the United States, 444 from other Organisation for Economic Cooperation and Development (OECD) countries, 1039 from developing nations, and 505 from countries with reputations as tax havens. This does not, of course, represent every incorporation services provider, but the sample size is sufficiently large for the purposes of this Article.

We conducted two experiments using this pool of providers. First, we sought to test the effectiveness of international transparency law—particularly FATF regulations—using a pool of 2051 firms that included 63 U.S. firms and all of the non-U.S. firms. Second, we subjected the remaining 1722 U.S. firms to the same FATF conditions but also presented additional conditions, including a treatment to test the effectiveness of IRS regulations on provider behavior. In both experiments we also explicitly tested the ease with which customers who match the profile of terrorists could incorporate anonymously. All of these conditions are explained below.

Next, to complete each of these experiments, we randomly assigned and sent emails that were embedded with different experimental conditions. Before discussing how these treatments differed, we first note that each email shared several common features: (1) each was sent from a fictitious customer seeking a consultant; (2) each provided a rationale for wanting a shell company (including reduced liability and confidentiality); and (3) each asked about cost and identity document requirements. Beyond these commonalities, each email was specifically crafted to test compliance with either an international or domestic regulation. Furthermore, the emails allegedly originated from various areas of the world ranging from low-corruption OECD nations[175] to nations that are often associated with terrorism. The recipient firm was thus able to decide to either comply or refuse to comply with transparency standards.

1. Placebo

The first email was our "placebo" or baseline condition,[176] which was sent from one of eight smaller, wealthier countries. Several factors made the

[175] The OECD includes twenty original countries, including those listed in the text and other relatively wealthy countries such as the United States and the United Kingdom. *See* LIST OF OECD MEMBER COUNTRIES—RATIFICATION OF THE CONVENTION ON THE OECD, http://www.oecd.org/general/listofoecdmembercountries-ratificationoftheconventionontheoecd.htm (last visited Jan. 24, 2014).

[176] *See* Appendix A.

placebo emails appear the least suspicious. First, the placebo emails hailed from relatively low-corruption OECD countries with conceivably less risk of terrorist influence. These placebo countries were Australia, Austria, Denmark, Finland, the Netherlands, New Zealand, Norway, and Sweden—each listed as among the least corrupt countries on Transparency International's Corruption Perceptions Index (CPI).[177] For convenience, we refer to them collectively as "Norstralia." The variety of placebo countries ensures that a negative means event—for instance, a lurid transnational financial crime story or a government scandal—might bias results. Therefore, other than asking for anonymous incorporation, the placebo email does not contain anything especially suspicious. Where the email hailed from a non-English speaking nation, we injected spelling, syntax, or grammar errors to enhance authenticity. This placebo email served as a benchmark with which to compare response rates and requests for identity documentation under the remaining conditions.

Including the placebo, we examined twelve different conditions, four of which we report in this Article and summarize in Table 1.

Table 1: Summary of Treatments

	Key Features
Placebo	Alias originates from low-corruption, minor-power "Norstralia" country.
Terrorism	Alias claims citizenship in one of four nations associated with terrorism and purports to work in Saudi Arabia for an Islamic charity.
FATF	Alias notes that the FATF requires identification.
IRS	Alias notes that the IRS enforces disclosure requirements (for U.S. firms only).

177 *Corruption Perceptions Index 2012*, TRANSPARENCY INT'L, http://www.transparency.org/cpi2012/results (last visited Jan. 24, 2014). We excluded other top ten CPI countries, such as Switzerland and Singapore, because they are associated with financial secrecy or other tax-haven conditions. Interviews and other corporate sector materials indicate that a prospective client's country of residence and business sector are the primary indicators of risk to the finance industry. *See, e.g.*, KPMG INT'L, GLOBAL ANTI–MONEY LAUNDERING SURVEY 2007, at 25 fig.11 (2007), *available at* http://us.kpmg.com/microsite/fslibrarydotcom/docs/AML2007FULL.pdf (indicating, graphically, important factors banks consider under a "risk-based approach" when they are approached by a potential client).

2. Terrorism Treatment

In the second treatment, we posed as terrorist risks.[178] The aliases purported to consult for Islamic charities, work in Saudi Arabia, and originate in countries recognized as sites of suicide terrorism—Lebanon, Pakistan, Palestine, and Yemen.[179] In this treatment, we tested the effectiveness of two of the FATF's recommendations: the warning against "[c]ountries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organisations operating within them"[180] and the requirement that companies screen "[c]harities and other 'not for profit' organisations which are not subject to monitoring or supervision."[181] The combination of individuals (1) coming from a country perceived as a host to terrorists, (2) working for an Islamic charity, and (3) seeking financial secrecy should present a very obvious terrorist-financing risk.

3. FATF and IRS Treatments

Our FATF treatment adds to the basic control template a straightforward reference to the FATF.[182] As with the control template, the email purportedly originates from one of the eight "Nostralia" countries, but here, the fictitious consultant directly references FATF provisions that require the production of identification to create a shell corporation.[183] However, after referencing the provisions, the consultant reaffirms a desire for anonymity and asks what documents are actually needed.

We developed this treatment to test the international law and relations theories of managerialism[184] and legalization.[185] These theories imply that noncompliance results from either ignorance of the law or ignorance of the conditions under which the law applies. Accordingly, we would expect to see

---

178 *See* Appendix B.

179 *See generally* ROBERT A. PAPE, DYING TO WIN: THE STRATEGIC LOGIC OF SUICIDE TERRORISM 253-64 app. I (2005) (cataloging the date, weapon, location, and death toll of suicide terror attacks from 1980 to 2003).

180 FATF, GUIDANCE ON THE RISK-BASED APPROACH TO COMBATING MONEY LAUNDERING AND TERRORIST FINANCING 23 (2007), *available at* http://www.fatf-gafi.org/media/fatf/documents/reports/High%20Level%20Principles%20and%20Procedures.pdf.

181 *Id.* at 24.

182 *See* Appendix C.

183 *See id.* at 26.

184 *See generally* Kal Raustiala & Anne-Marie Slaughter, *International Law, International Relations and Compliance*, *in* HANDBOOK OF INTERNATIONAL RELATIONS 538 (Walter Carlsnaes, Thomas Risse & Beth A. Simmons eds., 2d ed. 2002). For a more detailed discussion of managerialism in the context of the results from our experiment, see *infra* note 201.

185 *See generally* Kenneth W. Abbott & Duncan Snidal, *Hard and Soft Law in International Governance*, 54 INT'L ORG. 421 (2000).

high rates of compliance in response to this condition because the email both invokes the relevant law and suggests that this specific context is one in which it applies.

The next treatment—the IRS treatment—builds upon the FATF treatment by additionally mentioning the possibility of IRS sanctions in the case of noncompliance.[186] Although the IRS does not enforce identity reporting requirements, its website lists the agency as an FATF partner,[187] and we included this information to see if it would act as an additional deterrent. Our expectation was that the additional information would raise the proportion of providers insistent on compliance and lower the number of those willing to do business, noncompliance notwithstanding.

B. *Coding the Responses*

1. Compliance Coding

After sending out emails according to the aforementioned protocol, we coded five types of responses to measure treatment effects: (1) no response, (2) refusal, (3) compliant, (4) partially compliant, and (5) noncompliant.

Some typical responses identified the email as a possible scam,[188] while others arguably sought more information and requested a higher premium.[189] A complete lack of response, which could have occurred for a number of reasons, was coded as "no response." When corporation service providers (CSPs) simply refused service, irrespective of the stated reason, we coded the responses as "refusal."

To be "compliant," a CSP must have asked for specific government-issued photo identification, whether notarized or certified. The requests generally involved a notarized photocopy of a passport picture page, which the CSP would store should law enforcement or regulatory officials demand documentation.[190]

"Partially compliant" CSPs requested some form of identification, but did not request notarized copies of government-issued identity documentation.[191] "Noncompliant" CSPs were those that offered to assist in forming an anonymous shell corporation without requiring any photo identification whatsoever.[192]

---

186 *See* Appendix D.

187 IRS, *International Investigations—Criminal Investigation (CI)*, http://www.irs.gov/uac/International-Investigations-Criminal-Investigation-(CI) (last updated Nov. 14, 2013).

188 *See* Appendix E.1 (Indignant Response).

189 *See* Appendix E.2 (Greedy Response).

190 *See* Appendix E.3 (Compliant Response).

191 *See* Appendix E.4 (Partially compliant Response).

192 *See* Appendix E.5 (Noncompliant Response).

To ensure that responses were coded accurately and consistently, each response was coded twice by separate researchers using a formal manual. In the case of discrepancies, a senior researcher arbitrated the codes and assigned them a final designation.

2. Random Assignment

This experiment's objective was to determine what factors make a CSP more or less likely to comply with international and domestic regulations on the formation of shell companies. Treatments were randomized, like in any other randomized experiment, to neutralize variation caused by confounding factors. Like patients in a randomized medical trial, the CSPs were randomly distributed to each of the different treatments. Because of the large pool of CSPs, we could reasonably expect that extraneous factors were balanced and, therefore, any changes to the outcomes would be due to the experimental conditions. In this way, we could accurately measure differences against the initial control group and correctly attribute differences in compliance rates to the singular factor we drew out in each of the treatments.

C. *Results and Findings*

1. Brief Summary of Compliance Rates

After we sent our treated emails and coded the responses, three key findings emerged from the study.

First, emails that presented a heightened risk of terrorism were, at least in part, an effective deterrent to noncompliance. Indeed, it was the most effective treatment in our study. Yet it raised plenty of cause for concern, especially because it produced mixed results, decreasing both noncompliance (good) and partial compliance (bad).

Second, we found that including information on international and domestic regulations had much less of an impact than we had anticipated. While the mention of U.S. regulations actually increased compliance, mentioning international regulations had no measurable impact.

Third, compliance within countries and U.S. states was inconsistent with any international relations theory. Compliance rates varied drastically from country to country, as well as among the individual U.S. states, independent of wealth or level of development. States with lax financial regulations, such as Wyoming and Delaware, were the worst offenders in the sample. They made (with relatively little hesitation) offers to assist in forming shell companies, regardless of the risks involved and the information

provided. Surprisingly, countries that are notoriously known as tax havens were actually some of the most compliant countries in our study. And tax havens as a group far outpaced OECD countries in compliance with international financial transparency standards.

2. Complete Discussion of Findings

We categorize our findings into five main sections: (1) overall effectiveness of know-your-client (KYC) rules requiring identity documentation, both among all countries generally and specifically among U.S. CSPs; (2) relative compliance rates among tax havens, OECD countries, and developing nations; (3) (in)sensitivity of CSPs to terrorism risks; (4) effect on compliance rates when CSPs were given more information about the rules and penalties for noncompliance; and (5) relative compliance rates among individual states within the United States and possible explanations of the disparate results.

In describing the compliance rates in each of these categories, we also refer to a "Risk Aversion Level" that measures the average number of CSPs we had to approach within a given subset of providers before we received a noncompliant offer to incorporate anonymously. Thus, if the noncompliance rate was five percent, the Risk Aversion Level would be twenty. Lower Risk Aversion Levels indicate that it was easier to find noncompliant CSPs. Very high Risk Aversion Levels often exist alongside very high rates of compliance (e.g., the Cayman Islands), very high rates of partial compliance (e.g., Denmark), very high rates of refusal and nonresponse (e.g., Utah), or some combination thereof. Thus, a high Risk Aversion Level could be attributable to a combination of these different patterns.

Basic FATF requirements mandate that authorities have "adequate, accurate, and timely information on the [real,] beneficial owners[]" of any given shell company.[193] Compliance with this rule is essential to fight a range of financial crimes and combat terrorism, and CSPs comply with this rule only if they collect fundamental identity documents. Yet before our experiment, policymakers had no data about the extent to which the requirements are actually followed.[194]

a. *Overall International Know-Your-Client Effectiveness*

Our results demonstrate low effectiveness of international and domestic KYC laws, particularly within the United States. When compliance is

193 FATF, *supra* note 169, at 22.

194 The only compliance information available has been FATF audits and reports submitted to the FATF by signatories.

measured across all countries for the placebo condition (1112 inquiries in the international sample, 816 emails in the U.S.), the noncompliance level for the international sample, including the 63 U.S. firms, is 8.7%. This translates to an overall Risk Aversion Level internationally of 11.5. The compliance rate includes nonresponses in the denominator, since some CSPs may fail to reply deliberately—thus complying with international law in a "soft" way.[195] In contrast, the noncompliance level for the placebo condition in the U.S. sample is 11.3% and the Risk Aversion Level is therefore 8.8, more than 20% worse than in the international sample. This demonstrates that creating an anonymous shell company is, quite possibly, easier in the United States than in most other countries.

However, this gap is likely widened by two main factors. First, there is a higher nonresponse rate from U.S. CSPs in the sample (78.0% compared to 49.1% in the international sample). The proportion of U.S. providers who replied to our inquiries *and* required no identity documentation whatsoever was 41.5%, which is roughly *two-and-a-half times* the 16.5% average in the international sample. To test the behavior of those firms that failed to reply, we sent a second email from a Norstralia alias simply asking if the firm was still in business and assisting customers but making no mention of confidentiality, taxes, or liability. The results show that the vast majority (83% internationally and 94% in the U.S.) of nonresponsive CSPs are not soft refusals—instead, they fail to respond to any inquiry, even the most innocuous request.

Second, there is great disparity in compliance rates between U.S. business law firms and other U.S. CSPs.[196] Business law firms replied at much lower rates than other CSPs (15.9% in the domestic and 41.8% in the international sample). The other, non–business law firm CSPs were also especially unlikely to ask for identity documentation. In fact, only a tiny proportion of U.S. providers actually met the more stringent international identity requirements (9 of 1722 U.S. providers, or 0.523%). Overall, U.S. business law firms were much less likely to violate international laws that prevent the funding of terrorism—mostly by refusing service.

---

[195] Internationally, 49.1% of our approaches did not generate a reply. The ratio was even higher in the U.S. sample at 78.0%, and U.S. law firms were highest at 84.1%. What does this high level of nonresponse mean for our results? This could be considered "soft compliance" because a provider thought the request was too suspicious. If this is generally true, most of the nonresponses could be judged as evidence of a functioning regulatory framework. On the other hand, if nonresponses bear no relation to de facto risk screening and are merely a product of commercial decisions, uninterest, or disorganization, then nonresponses cannot be regarded as evidence of a functioning regulatory system.

[196] *See infra* Figure 2.2.

Figure 1.1: International Risk Aversion Level by Treatment[197]

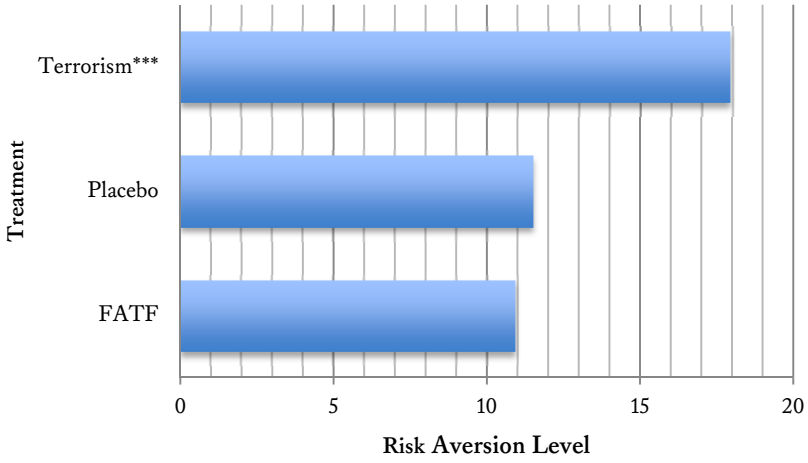
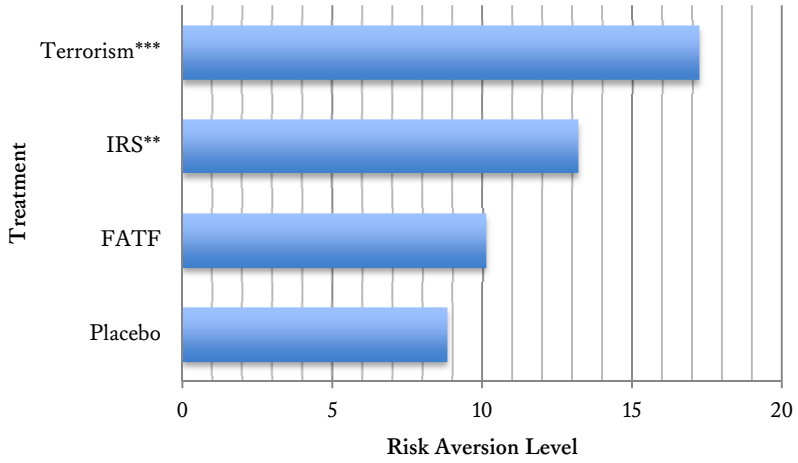


Figure 1.2: Domestic Risk Aversion Level by Treatment[198]



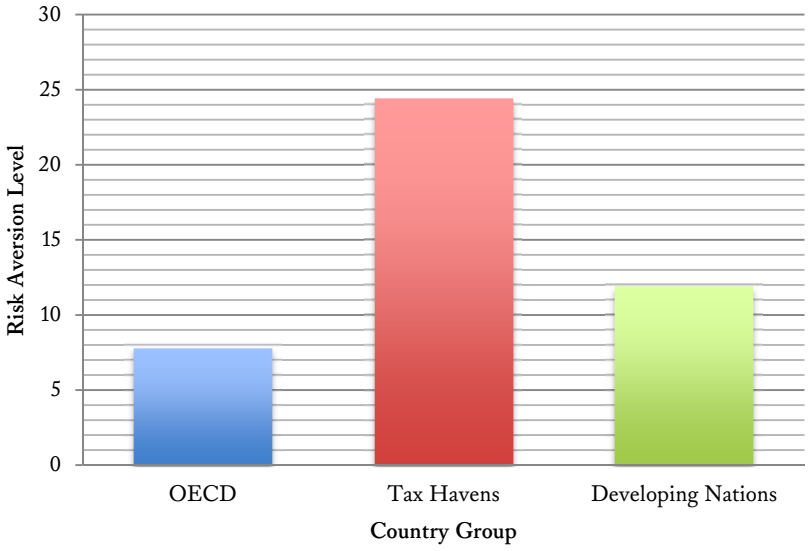
[197] International and U.S. results are reported separately. Asterisks denote statistical significance: ***p < 0.01 in two-tailed–difference-in-mean tests compared to the placebo.

[198] Asterisks denote statistical significance: ***p < 0.01; **p < 0.05 in two-tailed–difference-in-mean tests compared to the placebo.

b. *Relative Compliance Rates Among Countries*

A country's relative wealth seems to have no impact on its likelihood to enforce international laws that prevent the funding of terror. In our experiment, wealthy OECD countries (including the United States) were actually the least compliant with international identity incorporation requirements. This runs counter to the conventional wisdom that poor countries would be least compliant.[199] For developing countries, the average Risk Aversion Level is 11.9, whereas for OECD countries it is 7.8 (and, for tax havens, it is 24.4). This finding is significant because it demonstrates that enforcing identity requirements might not be expensive, since poorer countries fare better on average.[200] Thus, countries might fail to comply because of an *unwillingness* to enforce the rules, rather than any kind of *incapacity*, as some experts have posited.[201] In fact, incorporation services (excluding law firms) in the United States are the least compliant of those in any country with which we communicated more than fifteen times.

Figure 2.1: Risk Aversion Level by Type of Country Internationally

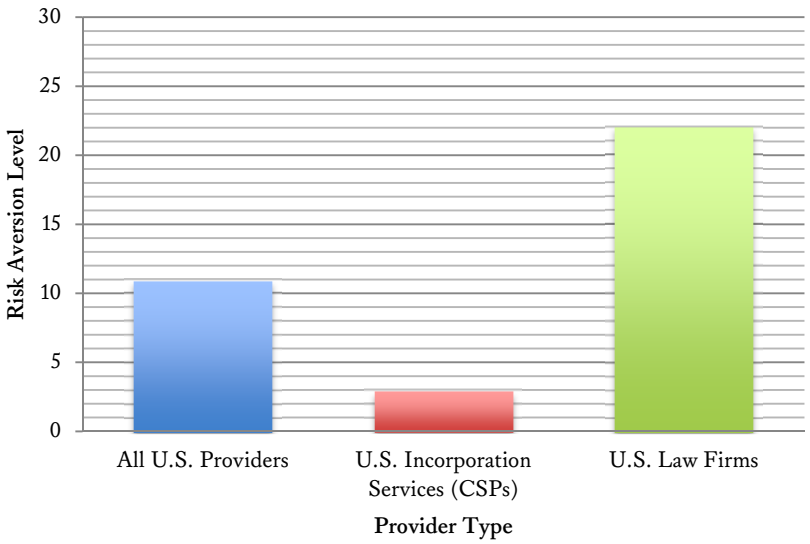


199 *See infra* Figure 2.1.

200 *See generally* Baradaran et al., *supra* note 172.

201 These findings contradict the managerial theory, which states that noncompliance results from a lack of resources and information. Abram and Antonia Chayes, central proponents of this theory, argue that the best way to "manage" compliance is to provide states with information and resources, rather than to threaten sanctions. Abram Chayes & Antonia Handler Chayes, *On Compliance*, 47 INT'L ORG. 175, 204-05 (1993).

Figure 2.2: Risk Aversion Level by Provider Type



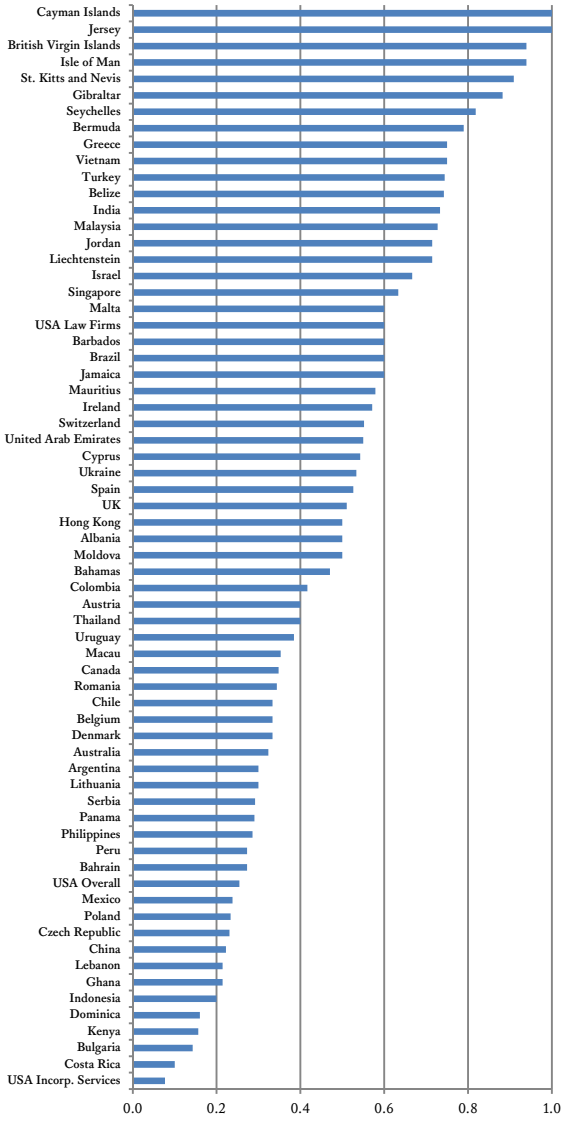
This finding contradicts the overwhelming consensus that tax havens provide secrecy and have lax regulation, particularly for shell companies. This traditional conception of tax havens is articulated by G20 communiqués, NGOs, and the U.S. media.[202] However, service providers located in tax havens made it surprisingly more difficult to form anonymous shell companies than those in OECD countries and developing nations. In fact, tax havens were more compliant than any other country group, with a Risk Aversion Level of 24.4—much higher than the OECD score of 7.8. This means that it was over three times more difficult to establish an untraceable shell company in a tax haven than in an OECD country. Some of these tax havens, including Jersey, the Cayman Islands, and the Isle of Man, are among the most compliant in the world, while OECD nations such as the United Kingdom, Australia, Germany, and the United States rank near the bottom (see Figure 3). It is also important to note that our experiment does

202 *See, e.g.*, Christopher Matthews, *The Real Problem with Offshore Tax Havens*, TIME (July 26, 2012), http://business.time.com/2012/07/26/the-real-problem-with-offshore-tax-havens (noting the common notion of (offshore) tax havens as "sun-drenched islands ruled by corrupt governments in cahoots with felonious plutocrats"); Robert M. Morgenthau, *These Islands Aren't Just a Shelter from Taxes*, N.Y. TIMES, May 6, 2012, at SR8 ("The secrecy laws in these tax havens are at the root of serious crimes: fraud, money laundering and international terrorism."); *cf.* Stephen Troiano, *The U.S. Assault on Swiss Bank Secrecy and the Impact on Tax Havens*, 17 NEW ENG. J. INT'L & COMP. L. 317, 345-46 (2011) (explaining that "a responsible and fair system needs to be implemented in order to curb the abuse of tax havens . . . through multilateral action").

not consider tax havens compliant unless they explicitly require notarized identification for beneficial owners of the company, which helps to avoid legal fictions. [203]

[203] For a description of how corporations and shell companies disguise beneficial ownership, see Azam Ahmed, *In Caymans, It's Simple to Fill a Hedge Fund Board*, N.Y. TIMES DEALBOOK (July 1, 2012), http://dealbook.nytimes.com/2012/07/01/in-caymans-its-simple-to-fill-a-hedge-fund-board.

Figure 3: Compliance Rate by Country for Nations with at Least Twenty-Five Approaches[204]



204 The bar chart reflects the overall compliance rate, where firms demanding notarized photo ID and refusing service are together shown as a proportion of all firms responding to inquiries. Countries were included if we received more than twenty-five responses. All twenty-five U.S. firms from the U.S.-only sample (Figure 4) are included with the sixty-three U.S. firms in the international sample.

c. *(In)Sensitivity to Terrorism Risks*

Our terrorism treatment produced mixed results. To begin, customers shopping under this treatment were less likely to receive a reply. In fact, nearly 60% of requests in the international sample and more than 80% in the domestic sample received no response, which suggests a significantly greater number of "soft" refusals compared to the placebo. Also, the results demonstrate that the terrorism treatment causes significantly lower non-compliance rates compared to the placebo, which suggests that it is more difficult for potential terrorists to incorporate anonymously.[205]

However, the terrorism treatment also decreased the rate of partial compliance in the international pool. Firms were less likely to ask possible terrorists for at least some non-notarized form of identification compared to the placebo condition. For instance, the partial compliance rate in the international sample was only 11.1% for the terrorism condition compared to 16.6% with the placebo. This result may indicate that the level of risk tolerated by a large number of firms is higher with the terrorism treatment than with others. Furthermore, firms that recognize the terrorism red flags may actually want to be left in the dark about client identity to avoid potential liability.[206]

The results were similar in the U.S. sample. Potential terrorists received fewer refusals when compared to the international sample. However, in contrast to the international sample, virtually no firms asked for supporting identification in the United States. The only way U.S. firms complied with FATF standards was through refusals. It is thus particularly worrisome that the refusal rate dropped so dramatically in the U.S. sample. In other words, it was easier to form a terrorist organization in the United States than in the rest of the world—a result made more troubling when one considers the lower overall U.S. response rates. As a share of responses, U.S. CSPs were easily the most willing to form anonymous shells for individuals matching a terrorist

---

205 The federal government has made efforts to provide incorporation services providers information on "red flags" that indicate terrorist financing, which may have contributed to this finding. *See generally, e.g.*, FED. FIN. INSTS. EXAMINATION COUNCIL, *supra* note 16 (providing examples of "red flags").

206 In some ways, this is not surprising given the lax domestic regulation in many countries, including the United States. For one profound anecdote, see *All Things Considered: Shell Game: 2,000 Firms Based in One Simple House* (NPR radio broadcast July 2, 2011, 4:27 PM) (describing a home in Wyoming that houses 2000 shell companies with little oversight), *available at* http://www.npr.org/2011/07/02/137573513/shell-game-2-000-firms-based-in-one-simple-house. The desire for money is also at the heart of these results, because incorporation services providers stand to profit greatly and they are an integral part of many economies, including that of the Netherlands. Crouch, *supra* note 77.

profile. Certainly, it was harder to incorporate anonymously for the aliases in the terrorism condition than the others—but it still proved disturbingly easy.

Overall, the terrorism condition findings show that relying on CSPs to decline customers that pose a terrorism risk may not adequately deter terrorism financiers. Though riskier customers should receive heightened scrutiny, CSPs were ineffective at screening corrupt customers. In many cases, CSPs did not even require identifying information from customers posing an obvious risk of terrorism. As such, policymakers may want to reconsider a "risk-based approach" in domestic regulations and incorporation standards. Additional government oversight or domestic penalties may prove more effective in improving firms' scrutiny.[207]

d. *Effect of Additional Information: IRS*

We tested two different questions in the subsequent treatments: (1) whether informing providers about the rules makes them more likely to follow them (FATF treatment) and (2) whether raising the prospect of penalties makes providers any more likely to comply with KYC rules (IRS treatment). We found, in brief, that (1) information *does not* induce additional CSP compliance; and (2) priming CSPs with a reference to a well-known domestic enforcer *partially* induces compliance.

Our experiment demonstrated that informing firms about international laws requiring identifying information for clients did not increase adherence to those laws. There was little difference between the placebo (11.5 international, 8.9 U.S.) and the FATF treatments' Risk Aversion Levels (10.9 international, 10.1 U.S.). However, the prospect of IRS enforcement *significantly decreased* the noncompliance rate in the United States, thereby boosting the Risk Aversion Level from 8.8 (placebo) to 13.2 (IRS). These findings demonstrate two important points: (1) it is not ignorance of the law that causes global noncompliance; and (2) the threat of IRS enforcement (a possible domestic penalty) has a greater effect than knowledge of FATF standards (a potential international penalty).

---

[207] In the United States, a number of agencies are tasked with overseeing screening for transactions that have a high potential for involvement in terrorist financing. For example, the U.S. Commodity Futures Trading Commission (CFTC) and the U.S. Treasury, acting under the authority of the PATRIOT Act, have jointly issued final rules regarding identity verification programs and requirements. U.S. ANTI–MONEY LAUNDERING, CFTC, http://www.cftc.gov/industryoversight/antimoneylaundering/index.htm (last visited Jan. 24, 2014).

e. *Variation Among U.S. States*

There was considerable variation among the individual U.S. states concerning identity requirements. Wyoming, Delaware, and Nevada were among the worst in compliance rates—demonstrating that providers in these states are most likely to sell untraceable companies to foreign clients.[208] The U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN), recently chided these states, as well as Oregon, for being "particularly appealing" locations to form shell companies.[209] It comes as no surprise that these states have some of the worst compliance rates because, as discussed previously, they also have the most lax identity requirements for forming a shell company.[210] Yet a more careful analysis of the states we found to be most and least risk-averse is in order.

Why do states continue to allow lax identity-reporting requirements despite the accompanying risks of corruption and terrorism? One answer is large profits. Cyrus R. Vance, Jr., District Attorney for Manhattan, recently observed: "Secrecy [in forming shell companies] has become a big business."[211] In fact, many major U.S. corporations, including Exxon, Chevron, and Rio Tinto, use a number of Delaware subsidiary companies to transact business.[212] However, there is not enough federal involvement to prevent this longstanding practice.[213] While legislation such as the ITLEA[214] would allow the federal government to require states to impose more thorough identity reporting requirements, it has continually been blocked in congressional committee.[215] Moreover, while federal regulation is one way to increase

---

208 *See infra* Figure 4 (Compliance Rate by State).

209 *See* Wayne, *supra* note 149. FinCEN also noted that Delaware is the worst offender. *Id.* The U.S. Treasury, together with multiple agencies including the IRS, has formed a working group to assess the threat of money laundering. DEP'T OF THE TREASURY, U.S. MONEY LAUNDERING THREAT ASSESSMENT (2005), *available at* http://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/mlta.pdf. Unsurprisingly, one of the working group's reports noted that shell companies and trusts were major areas of concern in states like Delaware and Wyoming. *Id.* at 47-50. As financial institutions across the United States are better informed regarding the threat of terrorist financing, and as they report suspicious activity more effectively (including through SARs), we hope that this activity will decline.

210 *See supra* notes 78-84 and accompanying text.

211 Cyrus R. Vance, Jr., *The Great Debate: It's Time to Eliminate Anonymous Shell Companies*, REUTERS (Oct. 9, 2012), http://blogs.reuters.com/great-debate/2012/10/09/its-time-to-eliminate-anonymous-shell-companies.

212 *See* Wayne, *supra* note 149.

213 *Id.*

214 Incorporation Transparency and Law Enforcement Assistance Act, S. 1465, 113th Cong. (2013).

215 *See S. 1483 (112th): Incorporation Transparency and Law Enforcement Assistance Act*, GOVTRACK, http://www.govtrack.us/congress/bills/112/s1483 (last visited Jan. 24, 2014); *supra* note 125 and accompanying text.

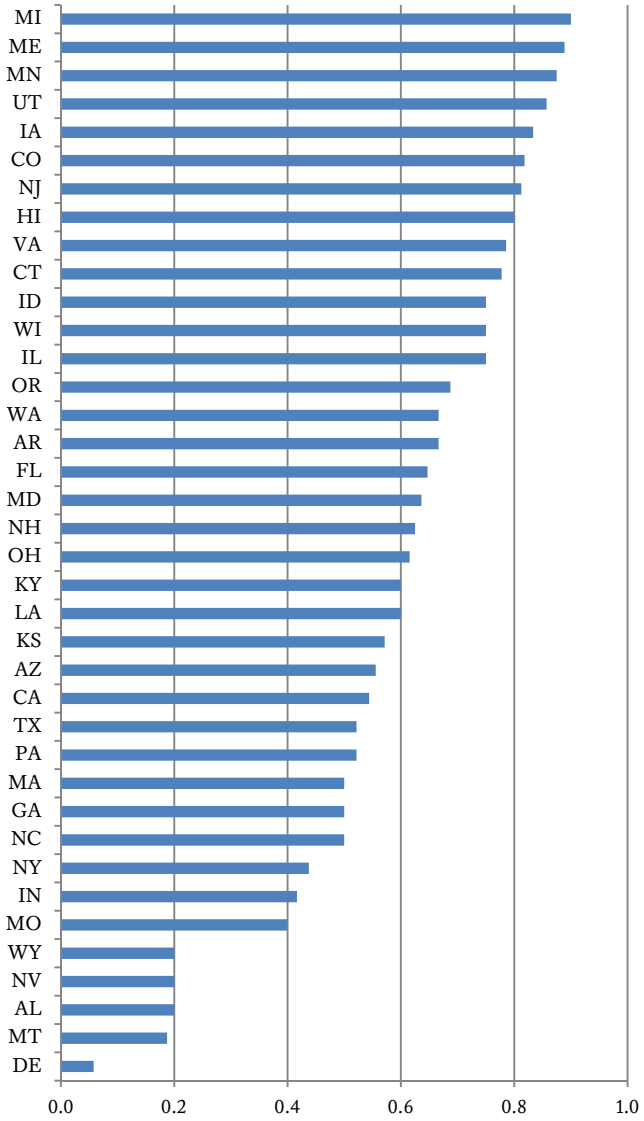
oversight, another may be to compare the oversight regimes of the least- and most-compliant states. In particular, the states found to have no instances of noncompliance—including Arkansas, Maine, Utah, and Minnesota—should be studied to determine if any specific regulations induced greater compliance.[216] At the very least, these results will be instructive to state policymakers interested in creating a business-friendly environment but wary of opening their doors to terrorism and corruption.

---

216 While there have not been studies comparing compliance among the various states, an FATF review of U.S. compliance with FATF regulations and domestic financial enforcement measures found that "[t]he law enforcement arena appears to be fragmented," partially due to overlapping jurisdictions and mixed roles for task forces. FATF, *supra* note 113, at 256-57. The report did note, however, that thirty-seven states, as well as the District of Columbia, have joined with the Money Transmitter Regulators Association (a nonprofit organization) to draft model legislation and regulate money-service businesses. *Id.* at 256.

Also, in a study of the role of shell companies in the various states, FinCEN noted that while "some states require the reporting of information on *ownership*, no state requires the reporting of information on *beneficial ownership*." FIN. CRIMES ENFORCEMENT NETWORK, *supra* note 16, at 3 n.2 (emphases added). FinCEN also found that fourteen of the states with the "least transparency" also had absolutely no requirement to report the identities of LLC members *or* managers. *Id.* at 9. Whether there is a more direct correlation between stringency of state regulations and ease of forming a shell company is a topic for further study and consideration.

Figure 4: Compliance Rate by State[217]



[217] Similar to Figure 3, the bar chart shows compliant and refusing firms together as a proportion of all responses. States were included if we received five or more responses to our inquiries from firms residing in the state.

III. THE FUTURE OF THE WAR ON FINANCIAL TERROR

The results of our international global field experiment demonstrate that domestic policies implemented in the war on terrorist financing have fallen short. International and domestic laws since 9/11 have worked to increase information sharing and have increased restrictions on the financial sector, but many firms are still willing to aid in forming anonymous shell companies. Our experiment challenges these laws by exposing the large gaps that exist between goals and practice.

Specifically, we tested the ease of forming an anonymous shell company without adhering to the identity requirements of universally accepted international laws. The results were disturbing. International laws requiring customer identification to form shell companies are not effective. Almost half of the companies we approached did not ask for *proper* identification, and twenty-two percent did not require *any* identity documents. We also found that knowledge of international laws does not increase the likelihood that firms will require identity information.

Our results further showed that forming an anonymous shell company capable of helping to finance terrorism is much easier within the United States than abroad. In fact, it was easier to form an anonymous shell company in the United States than in any other country.[218] Within the United States, the worst offenders of lax enforcement of international corporate transparency standards were Delaware, Wyoming, and Nevada—typically considered the most business-friendly states.

In combination, the above results are not good news for the current domestic and international regulatory framework. Shell companies are widely available and easy to procure. More developed OECD countries—including the United States and others that participate directly in the FATF—are some of the worst offenders of the identity reporting requirements, according to our study. We found that it is three times easier to form an anonymous shell company in an OECD country than in the oft-reviled tax havens. Surprisingly, tax havens as a group are the hardest places in the world to form anonymous shell companies.

On the other hand, U.S. firms were less likely to aid an individual seeking to form an anonymous shell company when we provided them with information about IRS regulations. In fact, stating that IRS regulations required disclosure (even though there is no such requirement) induced more compliance than mentioning the substantive international FATF recommendations—which had

218 *See supra* Figure 3 (Compliance Rate by Country). U.S. incorporation services ranked at the very bottom of our sample for risk aversion. U.S. service providers generally (including both law firms and incorporation services providers) still fell into the bottom third of all countries in the sample.

no effect at all. This empirical evidence supports incorporation of FATF recommendations—particularly more stringent identity requirements—into domestic regulations, as opposed to relying on the perceived weight of international standards.[219] Thus, our experiment leaves hope that increased domestic regulation and enforcement of international laws could improve compliance. Indeed, it is highly likely that tax havens perform so well because of vigilant domestic enforcement of international standards.

Our research suggests that governments must demonstrate a commitment to enforce international regulations and work more closely with the private sector if they wish to curb terrorism financing. Two important findings here demonstrate that close collaboration between governments and the private sector provides some hope. First, there is great variation among nations' compliance rates with international identity requirements, a fact that demonstrates different levels of commitment among governments throughout the world. Ironically, the countries that are most compliant are tax havens.[220] But upon further examination, this finding is not as surprising as it may seem. In tax havens, government regulators work very closely with private firms to enforce KYC regulations and other identity requirements.[221]

---

219 *See* 158 CONG. REC. S5093, 5104-05 (daily ed. July 18, 2012) (statement of Sen. Carl Levin) (calling for Congress to address tax havens and combat "offshore tax abuses"); FIN. CRIMES ENFORCEMENT NETWORK, *supra* note 16, at 14 (suggesting outreach to state governments to address "vulnerabilities in the state incorporation process"); Navin Beekarry, *The International Anti–Money Laundering and Combating the Financing of Terrorism Regulatory Strategy: A Critical Analysis of Compliance Determinants in International Law*, 31 NW. J. INT'L L. & BUS. 137, 155-93 (2011) (evaluating factors affecting FATF compliance); Bradley J-M Runyon, *Money Laundering: New Legislation and New Regulations, But Is It Enough?*, 3 N.C. BANKING INST. 337, 342-43 (1999) (explaining pre-9/11 deficiencies in domestic legislation regulating money laundering).

220 *See supra* Figure 3. Our findings strongly suggest that notorious tax havens like the Bahamas, the Cayman Islands, and the Isle of Man are actually quite compliant in terms of requiring identity documentation. However, the FATF placed these nations on its blacklist as recently as 2000. *See* Peter Lilley, *The FATF 'Blacklist*,' DIRTY DEALING, http://www.dirtydealing.org/IMAGES/fatfblacklist/The%20FATF%20Blacklist.pdf (last updated Mar. 2006); *see also* INL, *supra* note 53. Furthermore, these countries still carry a reputation as sites for money laundering, which may be partially due to political rhetoric. *See* Daniel J. Mitchell, *Tax Havens Are Not Money Laundering Centers*, CATO INST. (Feb. 19, 2010), http://www.cato.org/blog/tax-havens-are-not-money-laundering-centers.

Other studies, as well as the FATF's most recent categorization of "high risk" jurisdictions, do not list any of these so-called tax havens as high-risk countries. *See, e.g.*, *id.* (citing *Money Laundering and Terrorist Financing: High Risk Jurisdictions*, BASEL INST. ON GOVERNANCE, http://baselgovernance.org/fileadmin/docs/LISTE.jpg (last visited Jan. 24, 2014) (mapping "nations where there *actually* is a high risk of money laundering and terrorist financing" (emphasis added))); *see also* HIGH-RISK AND NON-COOPERATIVE JURISDICTIONS, *supra* note 133 (identifying jurisdictions with "strategic deficiencies," notably not including any tax haven countries as of October 2013).

221 This statement is based on author interviews with CSPs and government regulators at conferences in various locations in the tax havens. Additionally, officials in these nations have been very outspoken about their efforts to control money laundering and shell companies. *See, e.g.*,

These governments understand the importance of business clients and want to maintain a respectable reputation internationally for incorporation and banking.[222] With this close government oversight—and despite the negative press some tax havens have received over the years[223]—many maintained perfect compliance in our field experiment. Many others were nearly perfect.

By contrast, a number of U.S. states such as Delaware, Nevada, and Wyoming have abysmal compliance records. The United States' failure to enact domestic legislation that implements international requirements to promote identity transparency[224] has facilitated a race to the bottom. States appear willing to incorporate anyone—including, as our experiment demonstrates, high-risk clients.[225] The extremely low compliance levels of Delaware compared to those of the tax havens is most disconcerting. States like Delaware compete with tax haven nations to attract business clients, but they have chosen opposite approaches, with Delaware and similar states allowing noncompliance

---

Ambassador Curtis A. Ward, Caribbean Res. & Pol'y Ctr., Panel on National Security, Threat of Drugs, Terrorism and Smuggling at the Northern Caribbean Conference on Economic Cooperation: Security Imperatives for the Northern Caribbean (Dec. 17, 2010) (transcript available at http://www.caribbeanresearchandpolicycenter.org/publications/docs/Security_Imperatives_for_the_Northern_Caribbean.pdf) (proposing the adoption and implementation of "minimum security standards" to combat money laundering and terror financing). For example, officials in the British Virgin Islands have led a campaign with the private sector to foster development of legitimate businesses within the nation. *See* Livia Freeman, *British Virgin Islands*, IBA ANTI–MONEY LAUNDERING FORUM, http://www.anti-moneylaundering.org/northamerica/British_Virgin_Islands.aspx (last updated Nov. 1, 2010) (describing money laundering regulations and legislation in the British Virgin Islands).

222 Many of these countries have very recently enacted stricter legislation on shell company formation. For instance, the Isle of Man has given law enforcement greater power to conduct financial reviews when individuals are suspected of criminal activity. *See, e.g.*, *Isle of Man*, KNOW YOUR COUNTRY, http://www.knowyourcountry.com/isleofman1111.html (last updated Mar. 25, 2013) (detailing legislation to combat money laundering on the Isle of Man). Also, in 2007, Bermuda created the independent Financial Intelligence Agency (FIA) to investigate suspicious financial activity in the island nation. *See, e.g.*, FIN. INTELLIGENCE AGENCY BERMUDA, http://www.fia.bm (last visited Jan. 24, 2014).

223 *See, e.g.*, Steven Hsieh, *Offshore Tax Havens Robbed States of Nearly $40 Billion in 2011*, ALTERNET (Feb. 6, 2013), http://www.alternet.org/economy/offshore-tax-havens-robbed-states-nearly-40-billion-2011 (noting that tax havens cost U.S. states $40 billion in lost revenue in 2011, in addition to roughly $150 billion in federal revenue); John O'Callaghan & Rachel Armstrong, *New Rules, Tough Talk as Singapore Seeks to End Tax Haven Image*, REUTERS (Oct. 15, 2012), http://www.reuters.com/article/2012/10/14/us-singapore-tax-idUSBRE89D0GM20121014 (expressing Singapore's concern over its reputation as a "magnet for tax evaders" and highlighting actions it is taking to change that image).

224 As discussed above, Senator Levin has introduced the ITLEA in several previous Congresses, but the bill has failed to even emerge from committee. *See supra* note 215 and accompanying text. The bill was reintroduced on August 1, 2013, as S. 1465, and was referred to committee on the same day. *See S. 1465: Incorporation Transparency and Law Enforcement Assistance Act*, GOVTRACK, https://www.govtrack.us/congress/bills/113/s1465 (last visited Jan. 24, 2014).

225 In the domestic sample, nearly six percent of firms were still found noncompliant when a request was sent from a source with obvious indicators of terrorism. *See infra* Table 3.

and the tax havens collectively maintaining the strictest compliance with international regulations. Significantly, these findings suggest that greater compliance results from a government's higher level of commitment to international requirements and close collaboration with the business sector, even in states or nations that work competitively to attract business clients.

Greater government commitment is associated with a number of essential components of effective oversight, such as more stringent identity reporting requirements. Another component is informing financial institutions of KYC requirements and the criteria for "suspicious" transactions.[226] Of course, the financial sector may respond better if it is working *with* the government for the mutually beneficial goal of countering terrorism financing rather than merely complying with regulations.[227] But such efforts will be ineffective if the United States does not also work with other nations to avoid an international race to the bottom in enforcing identity requirements for the formation of shell companies.[228] As this study has demonstrated, a warning that the IRS requires identity documentation actually affected compliance rates, whereas a warning that international laws required identity documentation had no effect at all. These findings suggest that domestic regulation is far more effective than international regulation at enforcing identity requirements.[229] Though coordinated implementation of identity reporting requirements will undoubtedly prove difficult, domestic regulation is crucial if nations wish to prevent the funding of terror.

---

226 *See* Lacey & George, *supra* note 120, at 347 (suggesting that a transaction deemed "suspicious" could require that the parties provide additional information).

227 *See* Richard Barrett, *Time to Reexamine Regulation Designed to Counter the Financing of Terrorism*, 41 CASE W. RES. J. INT'L L. 7, 18 (2009) ("Financial institutions have as much interest in preventing terrorist attacks as any other sector of society . . . . All sides would benefit if the suspicious activity reports submitted by banks and similar bodies were based on real concerns of possible criminality rather than the fear of falling short of the regulators' expectations.").

228 International cooperation and uniformity are particularly important for anti–money laundering standards to fight terrorist financing. *See* Lacey & George, *supra* note 120, at 349-50.

229 To make international regulations more effective, we must "re-conceptualiz[e] the public good of open financial systems as having negative security externalities that must be collectively managed." Clunan, *supra* note 63, at 570-71. Collective management will be difficult, but one common suggestion is to have "a multilateral organization . . . draft a comprehensive anti-money laundering convention, and then have signatory nations to the convention adopt implementing domestic legislation." Lacey & George, *supra* note 120, at 349-50. Such a convention could

> diminish enforcement difficulties and facilitate cooperation between nations in enforcement by including provisions for domestic governments to obtain the necessary evidence to investigate and prosecute cases where the evidence is in a foreign jurisdiction. Formal monitoring procedures to track the compliance of signatories in adopting the necessary implementing legislation are a necessary component.

Id. at 350. This convention would, in turn, help increase compliance on the domestic front.

APPENDIX

A. *Placebo/Control*

Dear Rapid Filing Inc.:

I am a consultant in need of an international corporation. I am a Sweden resident and I operate my business here with two associate [sic]. I have contacted you because I have several international clients in your region. Recently, our business has grown and tax [sic] have become more burdensome.

Also I hope to limit my liability, and I think that incorporation is the best solution. I am eager to maintain business confidentiality and to keep the process as discrete as possible.

I would specifically like to know what identifying documents you will require and what the costs will be. Due to a heavy upcoming travel schedule, the best way to reach me will be via email.

I look forward to hearing from you.

[Alias]

B. *Terrorism Treatment*

Dear Incorporation Value Company:

My name is Ahmed Haddad. I am [sic] resident of Saudi Arabia and a Lebanese national and I consult for several businesses here, though we also have many international clients. We consult for a number of Muslim aid organizations.

I am contacting you because our business in your area has recently increasing [sic]. I have been exploring different options for the establishment of an international corporation. My business associates and I wish to incorporate for tax purposes and liability reasons. We also wish to limit disclosure of information as much as possible as we form this company.

What specific identifying documentation do you require for us to form this corporation? How much will the service cost? Due to my heavy travel schedule, email is the best way to reach me.

Thank you for your time.

[Alias]

C. *FATF Treatment*

Dear Incorporation Value Company:

I am contacting you regarding a business I am trying to set up. I am a consultant and my colleagues and I are seeking to establish an international corporation. I am a [Norstralia] resident, but I do business both locally and with some international client [sic], including some in your region. Our business has been growing substantially, and our goal is to limit tax obligations and business liability. We would like as much business confidentiality as possible in these early stages of formation. My Internet searches show that the international Financial Action Task Force requires disclosure of identifying information. But I would rather not provide any detailed personal information if possible.

So, we would like to know what identifying documents will be required to establish this company. We would also like to know what start-up costs will be. Due to my travel schedule, email will be the best way to reach me. I look forward to hearing from you soon.

Regards,

[Alias]

D. *IRS Treatment*

Dear Incorporation Value Company:

I am writing on behalf of myself and the other two associates of our small consulting business, currently based in [Norstralia]. We do work in your area, so my purpose in writing is to request assistance and direction on incorporation internationally—although we live and operate in [Norstralia], international incorporation is the best thing for our business right now since we are taking on more clients, and for tax purposes, as well as to limit liability. We would like to form a new company in your area as private individuals. Additionally, we'd like to make this process as private and confidential as possible. My Internet searches show that United States law, enforced by the Internal Revenue Service, requires disclosure of identifying information when forming a company. But I would like to avoid providing any detailed personal information if possible.

Can you please inform me which identification documents will be required by you and how much your services will cost? It will be much easier for you to reach me via email than on the phone.

Thanks in advance.

[Alias]

E. *Response Emails*

1. Indignant Response

Dear [Alias]

I am assuming that your email was completely fraudulent.

If I am incorrect and this is not the case, please contact me on the number below and I will endeavour to assist.

However, if you [sic] indeed your intention behind contacting me is to make a lazy, fraudelent [sic] buck at the expense of others, then please spare a thought for the prospect you will remain a complete, impoverished idiot for the reseof [sic] your life and die poor and sad.

I will be leaving you nothing in my will.

2. Greedy Response

Your started [sic] purpose could well be a front for funding terrorism, and who the f*** would get involved in that? Seriously, if you wanted a functioning and useful Florida corporation you'd need someone here to put their name on it, set up bank accounts, etc. I wouldn't even consider doing that for less that 5k a month, and I doubt you are going to find any suckers that will do it for less, if at all. If you are working with less than serious money, don't waste anybody's time here. Using a f****** google account also shows you are just a f****** poser and loser. If you have a serious proposal, write it up and we will consider it. Your previous message and this one are meaningless crap. Get a clue. Just how stupid do you think we are?

3. Compliant Response

Herewith, the requisite forms for your [sic] to complete. The identifying documents you must send are as follows: 1. Certified copies of the information pages of your passport or of your driver's license 2. Certified copies of two utility bills or other, showing your usual place or residence 3. Two

reference letters, one from a bank and the other form a business or other associate. Have these sent directly to us from [sic] the persons giving the same. Please remit half of the fee at this time (see wire instructions below).

4. Partially Compliant Response

Thank you for your enquiries. The Seychelles jurisdiction does not require disclosure of any documents and particulars of clients to any authority whatsoever save upon a Court Order for purposes of criminal investigation and money laundering. Your type of transactions that you wish to use the proposed company is ideal for a Seychelles International Business Company. This kind of company pays zero tax, does not require annual return of accounts, does not disclose the Directors and Shareholders. You can open a bank account in its name and make use of a credit card to access your funds as you wish. As your Registered Agent, we are required by Law to maintain details of our clients for our own protection. To incorporate the company we require scanned copies of your passport, proof of your residential address (not post office box address) by way of a utility bill drawn on your name and if it is in a non English language, it needs to be translated and notarized before a Notary in your country. Given the nature of your proposed business transactions, we are willing to offer our services for the sum of Euro 600 per year. This will include the following services: 1. Incorporation 2. Registered Office 3. Registered Agent 4. Opening of Bank Accounts is a separate service at Euro 200 per account. We trust you will find our quote reasonable and we look forward to hearing from you.

5. Noncompliant Responses

a. *Response 1*

We don't need a whole lot of info from you. You can place the order on our website under starting your company. It should only take 10 minutes and that is all the information we need from you.

b. *Response 2*

All that you need to do is to provide the name you want for your new company, that's it.

c. *Response 3*

We have many international clients with the same confidentiality concerns so I am happy to tell you that you have found the right service provider for your needs!

F. *Response Data*

Tables 2 and 3 below present the international and domestic compliance results. We cataloged responses as Noncompliant, Part-Compliant, Compliant, Refusal, or No Response. The tables also compare the compliance results across each of the treatments. Proportions that are statistically significant when measured against the benchmark placebo are indicated at the $p < .01$, the $p < .05$, and the $p < .1$ levels. The .01 level means, in essence, that there is 1/100 probability that the results were produced by random chance rather than by a meaningful treatment effect. The .05 level indicates a weaker significance, with the probability of the results being produced by random chance at 1/20. The .1 level indicates an even weaker significance, with the probability of variation being the result of random chance at 1/10.

Table 2: Experimental results by treatment and outcome category for the international samples[230]

Treatment	Total	Noncompliant	Part-Compliant	Compliant	Refusal	No Response
Placebo	1114	97	185	211	125	496
		(8.7%)	(16.6%)	(18.9%)	(11.2%)	(44.5%)
Terrorism	425	24**	47***	64*	43	247***
		(5.6%)	(11.1%)	(15.1%)	(10.1%)	(58.1%)
FATF	390	36	60	66	37	191
		(9.2%)	(15.4%)	(16.9%)	(9.5%)	(49.0%)

Asterisks denote statistical significance: ***$p < 0.01$; **$p < 0.05$; *$p < 0.1$ in two-tailed–difference-in-mean tests compared to the placebo.

230 In each cell, we include both the total number of observations and the associated percentage of CSPs.

Table 3: Experimental results by treatment and outcome category for the domestic samples[231]

Treatment	Total	Noncompliant	Part-Compliant	Compliant	Refusal	No Response
Placebo	816	92	13	3	106	602
		(11.3%)	(1.6%)	(0.4%)	(13.0%)	(73.8%)
Terrorism	550	32***	8	2	50**	458***
		(5.8%)	(1.5%)	(0.4%)	(9.1%)	(83.3%)
FATF	546	54	11	2	62	417
		(9.9%)	(2.0%)	(0.4%)	(11.4%)	(76.4%)
IRS	552	42**	12	2	54*	442***
		(7.6%)	(2.2%)	(0.4%)	(9.8%)	(80.0%)

Asterisks denote statistical significance: ***$p < 0.01$; **$p < 0.05$; *$p < 0.1$ in two-tailed–difference-in-mean tests compared to the placebo.

231 In each cell, we include both the total number of observations and the associated percentage of CSPs.