February 14, 2013

Rebalancing the Fourth Amendment

Shima Baradaran

Available at: https://works.bepress.com/shima_baradaran/8/
The events of September 11 forever changed the political and legal response to terrorism. After more than ten years, two wars, several targeted military strikes, and significantly increased surveillance, we still have not succeeded in stopping the growth of Al-Qaeda and other terrorist organizations. The war on terror has not just been a military one. To stop terrorism, it is imperative to cut off the flow of terrorism financing. To this end, a number of nations have created financial laws that prohibit the formation of anonymous companies and monitor suspicious bank transfers. These laws have been touted as evidence that we are winning the war on terrorism. This Article questions their efficacy. In particular, this Article proves how easy it is to form a terrorist finance network and exploits the impotence of both international and domestic financial regulations that have been passed in this area. The Article presents findings from the largest global randomized controlled trial 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 9/11. The results are disconcerting and demonstrate that we are much too far from a world that is safe from terror.

TABLE OF CONTENTS

I. THE DOMESTIC AND INTERNATIONAL WAR ON TERROR .........................10
   A. Financial Tools at Terrorists’ Disposal ......................................11
      i. Money Laundering .................................................................11
      ii. Charities and Trusts ..............................................................14
      iii. Shell Companies .................................................................16
   B. De-Funding Terrorism: Domestic Efforts .....................................20
      i. United States Military, Security, and Intelligence Efforts ............21
      ii. United States Financial Efforts .............................................25
   C. De-Funding Terrorism: International Efforts ..............................29
   D. Remaining Global Challenges ..................................................32

II. EXPERIMENTAL RESULTS ...............................................................35
   A. Design Study: Finding Providers, Composing Treatments ...............37
      i. Placebo ..................................................................................38
      ii. Corruption Treatment ............................................................40
INTRODUCTION

Financing—in particular, a secure financing network—is crucial for terror organizations.\(^1\) In order to finance its international operations, al-
FUNDING TERROR

Qaeda requires an estimated 30 to 50 million dollars per year. Establishing al-Qaeda’s financing network was in fact one of Osama Bin Laden’s earliest and most important accomplishments, because it provided millions in steady and secure income to the organization each year. Not every act of terrorism, however, requires terrorist organizations to expend great sums of money. For instance, the September 11th attacks cost al-Qaeda approximately $400,000-500,000, but the London transit bombings cost only about $15,000. Because terrorists can pull off enormously destructive attacks with very little money, a successful war on terror must reach deep into the financial heart of terrorism.

While 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 assets, and spent over $1.2 trillion since 9/11 on its major military operations abroad. The overall costs of fighting

3 INDEP. TASK FORCE, COUNCIL ON FOREIGN RELATIONS, TERRORIST FINANCING 2 (2002) [hereinafter CFR, TERRORIST FINANCING].
5 9/11 COMMISSION FINAL REPORT, supra note 2, at 169; 9/11 COMMISSION MONOGRAPH, supra note 4, at 3 (“The plot cost al Qaeda somewhere in the range of $400,000–500,000, of which approximately $300,000 passed through the hijackers’ bank accounts in the United States.”).
terrorism have compounded the national deficit, greatly impacted the financial markets, and one group of commentators has even called this fight the “three-trillion dollar war.” This is not to mention the other corresponding costs of terrorism, including the cost of security to civil liberties. Other nations have also spent billions, as the financial impact reaches far beyond our borders. The U.K., for instance, spends an estimated 3.5 billion pounds per year to fight terrorism. Because of these rising costs, many are concerned that while the United States has spent enormous sums on fighting terrorism with its military might, it has not invested sufficient resources in cutting off the true

15 See, e.g., Michael Jacobson & Matthew Levitt, Staying Solvent: Assessing Al-Qaeda’s Financial Portfolio 12, WASHINGTON INSTITUTE (Nov. 2009) (“Al-Qaeda has at times also resorted to more creative means of fundraising, including complicated internet-based transactions and cell phone solicitations.”); MARTIN WEISS, CONG. RESEARCH SERV., RS21902, TERRORIST FINANCING: THE 9/11 COMMISSION RECOMMENDATION 2 (“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.”).
FUNDING TERROR

lifeline of terrorism: its clandestine network of global financing. In particular, as this Article will examine in great detail, one of the most dangerous and accessible financial tools used by terrorists today is anonymous shell companies. These companies allow terrorists to disguise their identities, enabling them to covertly transfer funds towards illegal activity, even within U.S. banks. Shell companies pose particularly vexing problems for law enforcement as there is no way to trace an anonymous shell corporation back to any individual. Oftentimes, the only tangible remnant of a shell company is a P.O. Box—in other words, they are often “hollow” companies. Shell corporations do serve some legitimate purposes, such as facilitating mergers and international joint ventures, or serving as asset holding companies. However, due to their hollow nature,

---

16 CFR, TERRORIST FINANCING, supra note 3, at 2 (“Fundamentally, U.S. efforts to curtail the financing of terrorism are impeded not only by a lack of institutional capacity abroad, but by a lack of political will among U.S. allies. . . . Confronted with this lack of political will, the current administration appears to have made a policy decision not to use the full power of U.S. influence to pressure or compel other government to combat terrorist financing more effectively.”); see also RAPHAEL PERL, CONG. RESEARCH SERV., RL33160, COMBATING TERRORISM: THE CHALLENGE OF MEASURING EFFECTIVENESS 3 (2007) (noting how difficult it is to measure progress in fighting terrorism).


19 PUPPET MASTERS, supra note 18, at 35.

20 Id.; David Spencer, International Tax Evasion: Enablers and Shell Corporations, 18 J. INT’L TAX 36, 38 (2007) (some companies “have used more sophisticated cross-border schemes and/or investment structures . . . which go beyond legitimate tax minimization
they are commonly used as vehicles for corruption, money laundering, and more recently, terrorism. Although many of these organizations seem harmless at the frontend, posing as charities or legitimate businesses, these corporations are often involved in illicit activity and often lead law enforcement to a dead end, leaving them helpless to track the perpetrators.21

In an effort to combat terrorist financing, policy makers have begun identifying vulnerabilities in financial institutions and the ways in which terrorists have exploited them.22 New legislation has pushed for financial transparency as a measure to avoid corruption and terrorist financing within the United States and globally,23 but the effectiveness of these efforts is debatable given the ability of terrorist organizations to quickly adapt.24 And

21 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 (2009) (noting the easy path to secrecy, since “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.’”)(internal citation omitted); PUPPET MASTERS, supra note 18, at ix (“Law enforcement and prosecution cannot go after stolen assets, confiscate and then return them if they are hidden behind the corporate veil.”).


24 9/11 COMMISSION FINAL 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. DEPT. OF STATE, GAO-04-163, TERRORIST FINANCING: U.S. AGENCIES SHOULD SYSTEMATICALLY ASSESS TERRORISTS’ USE OF ALTERNATIVE FINANCING MECHANISMS
while others have commented about how easy it is to form an anonymous shell company, no study thus far has determined how effective domestic and international regulations have been at curbing their proliferation and use.

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. As the United States spends billions more each year on counterterrorism, understanding the effectiveness of these efforts is crucial. Of course, measuring the effectiveness of these efforts is increasingly difficult, and much of the rhetoric concerning successful U.S. intervention into the terrorism-financing network is simply political.

(Nov. 2003), available at http://www.gao.gov/new.items/d04163.pdf (“[Terrorists] move funds by concealing their assets through nontransparent mechanisms such as charities, informal banking systems, 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.”).


26 While this piece 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 CFR, TERRORIST FINANCING, supra note 3, at 18 (“International law enforcement cooperation has been slow, made inordinately difficult, or simply refused altogether. In no country—including the United States—are either Islamic charities or the underground hawala system effectively regulated.”).

27 See AVI JORISCH, Tainted Money: Are We Losing the War on Money Laundering and Terrorism Finance? (2009) (critiquing U.S. efforts at fighting terrorism financing); PAUL ROGERS, Why We’re Losing the War on Terror (2008) (evaluating the U.S. military terrorist response); Ahmed Rashid, Losing the War on Terror, WASH. POST (Sept. 11, 2006), http://www.washingtonpost.com/wp-dyn/content/article/2006/09/10/AR2006091001145.html (describing the serious threats that still exist, despite U.S. efforts). But see Jacobson & Levitt, supra note 15 (arguing that Al-Qaeda’s financial network is greatly debilitated); Press Release, U.S. Department of the Treasury, Assistant Secretary for Terrorist Financing David S. Cohen Remarks to the ABA/ABA Money Laundering Enforcement Conference (Oct. 12, 2009), http://www.treasury.gov/press-center/press-releases/Pages/tg317.aspx (“We assess that al Qaeda is in its weakest financial condition in several years, and that, as a result, its influence is waning.”); see also PERL, supra note 16.

28 Sue E. Eckert & Thomas J. Biersteker, (Mis)Measuring Success in Countering the Financing of Global Terrorism, in SEX, DRUGS, AND BODY COUNTS: THE POLITICS OF NUMBERS IN GLOBAL CRIME AND CONFLICT 247 (Peter Andreas & Kelly M. Greenhill, eds., 2010). Eckert and Biersteker note that while “there are no definitive metrics by which
Policymakers offer “perceptions of success” without offering data or even explaining their methodology. This Article seeks to provide a breath of fresh here—to deliver some 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 the disposal of terrorists. It pays particular attention to anonymous shell companies and discusses the laws that stop the formation of such companies, their shortcomings, and other 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 stop the threats of terrorism—both financially and militarily.

Part II describes and analyzes the results from our experiment, in which we pose as customers from around the globe seeking to form anonymous shell companies. During the course of our study, we sent over 7,000 requests to service providers around the globe asking for their assistance in forming anonymous shell companies. In some of the requests, we included obvious indicators of corruption and terrorism. In others, we tested whether knowledge of Financial Action Task Force, (FATF), and IRS regulations would impact the number of offers we received. On the whole, as will be described in greater detail below, the results were disconcerting. In particular, the knowledge of domestic and international law was much less of a deterrent to forming shell companies than would be hoped for. Indeed, our results place the efficacy of these financial regulations into question as a deterrent to funding terrorism.

Part III uses these results to answer some important questions. Are there certain countries or blocs of countries most likely to form fronts for terrorism? For instance, are offshore states (i.e. tax havens) more of a problem with allowing anonymous companies to form? Are poor countries more likely than rich countries to foster terrorism financing? Is domestic law more of a deterrent or international law in stopping the formation of such companies in the U.S.? The Article then concludes with some important lessons that can help U.S. regulators and the international community to stop the potential for billions in damage worldwide and mitigate the treats of future terrorism.

success or effectiveness can be assessed“ in this domain, there are still “a variety of information and indicators that can help paint an overall picture.” Id. at 260. They also describe how effectiveness can be difficult to measure because much of the valuable information and data to analyze is classified. Id. at 258.

29 Id. at 256.
FUNDING TERROR

I. THE DOMESTIC AND INTERNATIONAL WAR ON TERROR

In the days following the September 11th attacks, the United States took immediate steps to secure its borders, engage its military, and expand the scope of its intelligence efforts. As previously noted, these efforts have been so extensive that some analysts estimate that fighting the war on terror has cost the United States over 3 trillion dollars. Though not without its failings, the United States’ military and intelligence communities responded swiftly to disrupt terrorist activity at home and abroad. In addition to its military and intelligence response, the United States has also taken steps to “aggressively target Islamic terrorism’s financial infrastructure.” These efforts spanned the globe as the United States reached out to other nations and organizations to assist in its goal of

---


31 See Carter & Cox, supra note 11.

32 John Mueller & Mark Stewart, The Terrorism Delusion: America’s Overwrought Response to September 11, 37 INT’L SEC. 81 (Summer 2012) (describing how disproportionate and costly America’s response has been to Al Qaeda compared to the actual threat that Al Qaeda poses).


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 11th, including increased intelligence activities, law enforcement coordination, and increased 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—this included 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 Financial Action Task Force (FATF). Id. at 13.
FUNDING TERROR

preventing terrorism financing in domestic and world markets.\(^{35}\) But as the United States has worked to dismantle these terrorist financing networks, the terrorists have begun to adapt—in order 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 utilized by terrorists to finance their operations, with a particular focus on shell companies. It then summarizes domestic and international responses to the threat of terrorist financing, and compares the U.S. efforts with those of the international community. Finally, it parses out the shortcomings in those policies and what domestic policies might actually be promoting and furthering the use of shell companies as a front for terrorism and other illicit activities.

A. Financial Tools at Terrorists’ Disposal

Terrorists use a variety of means to fund their activities, including money laundering, charities, trusts, and particularly shell companies.

1. Money Laundering

First, 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 mask the income to make it appear

\(^{35}\) Id. at 13.

\(^{36}\) See Jacobson & Levitt, supra note 15 and accompanying text.

\(^{37}\) CFR, TERRORIST FINANCING, supra note 3, at 32.

This is a global problem, and it is estimated that between $590 billion and $1.5 trillion is laundered annually worldwide, some of which is used to fund terrorist organizations. Money laundering happens in three basic stages: placement, layering, and integration. At the placement stage, money obtained from illegal practices is deposited into a financial institution. The layering stage occurs when the money is “layered” through several financial transactions, which aids in covering up the illegal source of the funds. Shell companies are an important part of this process as funds are moved to supposedly legitimate companies. Finally, the integration stage involves putting the money back into economy, making the money appear to be legitimate.

Of particular concern are Informal Value Transfer Systems (IVTS)—utilized heavily in the Middle East and Asia. These non-conventional banking systems, through which money is transferred using a network of intermediaries, pose a real danger because of the anonymity and ubiquitous use for illegitimate funds transfers.

Much of the efforts in fighting financial terrorism since 9/11 have focused on combating money laundering, but challenges still remain for law enforcement. First, terrorists can launder money in a multitude of ways, including currency exchanges, stock brokers, casinos, automobile dealerships, insurance trading companies, gems and precious metals, internet banking, trusts, wire transfers, ATMs, mortgages, and brokerage.

---


43 DEP’T OF TREASURY FIN. CRIMES ENFORCEMENT NETWORK, ADVISORY: INFORMAL VALUE TRANSFER SYSTEMS (Sept. 1, 2010), http://www.fincen.gov/statutes_regs/guidance/pdf/FIN-2010-A011.pdf. Though IVT systems are used widely for legitimate transactions, they are particularly prone to abuse.


45 Johnson, supra note 42, at 9–10.
accounts—to name a few.\(^{46}\) Needless to say, the sheer variety of methods to launder money complicates the efforts of law enforcement.

Second, law enforcement has to combat a complex and well-financed set of laundering techniques. Traffickers constantly employ the latest technologies to keep ahead of law enforcement efforts.\(^{47}\) And third, the laws of various nations lack the consistency to effectively stop money laundering. Although most nations have enacted anti-money-laundering laws, some are stronger than others; subsequently, money launderers conduct business in the countries with the weakest laws.\(^{48}\) Indeed, “[t]he international money laundering effort is only as strong as its weakest link.” \(^{49}\)

2. Charities and Trusts

Though terrorists undoubtedly launder money through financial markets and other expected channels, terrorism is actually most heavily financed through legitimate means, such as charities and trusts. Because of the generally unregulated nature of these funds, terrorist exploitation of charitable and non-profit resources presents one of the most “serious challenges” for law enforcement.\(^{50}\) Specifically, terrorist organizations often exploit the principle of zakat, or charity, one of the five pillars of Islam.\(^{51}\)


\(^{47}\) Bachus, supra note 38, at 835 (citing Zagaris & Ehlers, supra note 46, at 1).

\(^{48}\) U.S, DEP’T OF STATE, 2012 INCSR: MAJOR MONEY LAUNDERING COUNTRIES (Mar. 7, 2012), http://www.state.gov/j/inl/rts/arcrit/2012/vol2/184112.htm (providing a list of “jurisdictions of primary concern” that are particularly vulnerable to money laundering “because of weak or nonexistent supervisory or enforcement regimes or weak political will”).

\(^{49}\) DO S NARCOTICS REPORT, supra note 46, at XII-63 to XII-71.


\(^{51}\) Ilias Bantekas, The International Law of Terrorist Financing, 97 AM. J. INT’L L. 315, 322 (2003) (“The source of zaka 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.”).
Charities elicit funding from a variety of sources, including membership fees, donations, sale of publications, and appeals to well-connected and wealthy members of the community.52

Another challenge for law enforcement—particularly within the United States—is that freedom of association and freedom of religion allow charitable and non-profit foundations to fund terrorism with less scrutiny and government interference.53 These groups have enjoyed particular success since the Cold War by appealing to religious and social commonalities.54 They have infiltrated engrained charities to hide their funding.55 Charitable funds are spent in a variety of ways to aid terror, including to “recruit terrorists, fund administrative activities of the organizations and support families of killed, arrested, or injured terrorists.”56 Unfortunately, many of these charitable organizations have been unaware that their funds were being used to support terrorism.57

In addition to charities, terrorists move money through trusts in order to take advantage of privacy laws that conceal information surrounding the formation of the trust.58 For example, “blind trusts” can be set up without reference to the parties or purpose of the trust.59 Also, some jurisdictions allow for “flee clauses” in the trust, which “enable[] the trust to be automatically shifted to another country if it prompts an inquiry.”60 The

52 Gardella, supra note 50, at 114.
53 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 (2006); see also Ruff, supra note 53, at 116.
54 Bantekas, supra note 51, at 321–22.
55 Victor Comras, Al Qaeda Finances and Funding to Affiliated Groups, in TERRORISM FINANCING AND STATE RESPONSES: A COMPARATIVE PERSPECTIVE 132 (Jeanne K. Giraldo & Harold A. Trinkunas, eds., 2007)
57 See Anne L. Clunan, The Fight Against Terrorist Financing, 121 POL. SCI. Q. 4, 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. Legitimate funds are commingled with funds destined for terrorists, making it extremely difficult for governments to track terrorist finances in the formal financial system.”).
58 Bantekas, supra note 51, at 323.
59 Id.
60 Id. (citing FATF, GUIDANCE FOR FINANCIAL INSTITUTIONS IN DETECTING TERRORIST FINANCING, ¶17 (Apr. 24, 2002), available at http://www.oecd.org/fatf/TerFinance_en.htm); See also Daryl Shetterly, Comment,
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. Islamic trusts have been implicated by the United Nations Security Council in a variety of terrorist acts, including bombings in India and arms dealing in Afghanistan.

3. Shell Companies

Finally, terrorists and many other nefarious organizations take advantage of shell companies to conceal and transfer money through bank accounts around the globe—including within the United States. Like with trusts, shell companies possess an important quality: identity protection. They obscure true beneficial ownership to the detriment of law enforcement worldwide. In fact, as the United States has pushed heavily to prevent money laundering and illegal money transfers, the use of shell companies has shown a corresponding increase.

A shell company is a business entity with no significant assets or ongoing business activities capable of transferring large sums of money


61 PUPPET MASTERS, supra note 18, at 20–23 (noting how difficult it can be to identify the true “beneficial owner” in trusts and other corporate arrangements”).


63 J. W. Verret, supra note 18, at 857 (“Law enforcement personnel assert that the use of corporate shell companies hampers their ability to investigate corporate suspects.”); Comras, supra note 55, at 124; Donato Masciandaro, Global Financial Crime: Terrorism, Money Laundering, and Off Shore Centres 239 (2004); PUPPET MASTERS, supra note 18, at 35–36.

64 They Sell Sea Shells, supra note 17 (“One reason for their ubiquity is an American-led push against money laundering.”).
They usually have no employees and lack any physical presence besides a mailing address. They are also easily formed, with many states not requiring ownership disclosure. They facilitate a variety of legitimate business purposes, such as “domestic and cross-border currency and asset transfers, . . . corporate mergers and reorganizations.” 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 take part in an estimated $1 trillion in transactions every year, and the taxes paid by these companies are an important source of revenue for the country.

Shell companies are so popular that an incorporation services industry has formed worldwide to cater to desiring clients. One of the most attractive characteristics is the privacy afforded by shell companies. One service provider in Wyoming advertises 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 cannot be held accountable for its actions. Imagine the possibilities!” Another such company in London promotes that Delaware is “an offshore tax haven for non-U.S. residents” and noted the advantages offered by such a company, including that “[o]wners’ names are not disclosed to the state,” and “the company is not required to report any assets.” Another Web site promotes that for under $70, it can create a corporation in Nevada, which “may provide for anonymous ownership and bearer shares.” Additionally, this site promotes “shelf” corporations, which are dormant incorporated businesses with a past operating history.

---

65 Krzysztof Woda, *The Analysis of Money Laundering Techniques* 141, in *CYBER WARFARE AND CYBER TERRORISM* (Andrew Colarik & Lech Janczewski, eds. 2008); *THE ROLE OF DOMESTIC SHELL COMPANIES*, supra note 21; see also *PUPPET MASTERS*, supra note 18, at 34 (defining a shell corporation as a “non-operational company—that is, a legal entity that has no independent operations, significant assets, ongoing business activities, or employees”).
66 *THE ROLE OF DOMESTIC SHELL COMPANIES*, supra note 7, at 2.
67 Id.
68 Id. at 4.
71 Elizabeth MacDonald, *Shell Games*, FORBES (Feb. 12, 2007), at 96
72 CORP95 PREMIERE INCORPORATING SERVICES, http://www.corp95.com/; see also id.
The popularity of these companies is so great, in fact, that in 2009, more than two million shell companies were formed in the U.S. alone. These shell companies offer an attractive medium for terrorists to move money anonymously around the world due to a lack of beneficial owner disclosure requirements and other lax regulations in many states. They can be used as a “back door” to the U.S. financial system, and allow terrorists, and their financial supporters, to evade sanctions. Indeed, many terrorist groups have capitalized on the potential of shell companies and have turned to the use of shell companies to launder and obscure their ties to illegal funds. Terrorist organizations can further distance themselves from the actual formation of a shell company by using a company formation agent to establish them, or by appointing puppet nominees to the leadership positions of the company so the true owners can hide their identities. Indeed, one expert opined that “of all the organizations employing money-laundering techniques, terrorist organizations are probably the most trained and adept at disguising their own origins as well as those of their funds.”

---

77 Id. (quoting Robert Werner, director of Treasury’s Office of Foreign Assets Control).
78 MacDonald, supra note 71, at 96 (Shawqi Omar, an American and Jordanian citizen was charged with plotting an aborted chemical attack on the Jordanian intelligence agency. Domestically, five of Omar’s relatives have been charged with using U.S. 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 --- Regulators Are Checking Alleged Links to Militants, Transactions to Charities, WALL ST. J., Feb 2, 2005, at B3. (The Arab Bank PLC, one of the Middle East’s largest banks, is currently under intense legal pressure in the U.S. over allegations that it is linked to Palestinian militant groups. According to government officials, U.S. bank regulators are investigating the Arab bank’s New York office for large-scale violations of money-laundering laws in connection with transactions made by Palestinian charities and others. Additionally, private lawyers for terrorism victims have also alleged that the Arab Bank PLC has financed Islamic militants, including suicide bombers).
80 Carr & Grow, supra note 70.
After the events of 9/11, however, the formation of shell companies and lax financial reporting laws were brought under increased scrutiny—particularly at the state level. Senator Levin, a principal proponent of reforms in this area, noted in a congressional hearing on the matter 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.” Due to these regulatory and oversight gaps, 1,002 Suspicious Activity Reports were filed with the Financial Crime Enforcement Network (FinCEN) between 1996 and 2005 identifying suspicious financial activity that appeared to be related to shell companies. 768 of these involved suspicious international wire transfers. Al Qaeda was aided by Osama bin Laden’s experience in money transfer techniques—that was his main area of technical specialization. In fact, Saudi officials discovered a network of over 50 shell companies used by bin Laden.

There is no simple mechanism, however, to detect and eliminate shell companies. State officials report that it would be too costly to investigate all the private companies seeking to incorporate and that disclosing the names of shareholders would violate businesses’ privacy. Another obstacle is that not all of a shell company’s assets are obtained through illegitimate means. The legitimate nature of many pools of terrorist funding poses difficulties for law enforcement officials working in a system that presumes that most funds used to support illegal activities are illicitly obtained. The aptitude of terrorists in moving and concealing their funds does not help the situation. The complex nature of transactions involving shell companies makes finding solutions to this problem difficult but there are critics who say that it is not as difficult as it may seem. “It’s not like we’re infiltrating

83 THE ROLE OF DOMESTIC SHELL COMPANIES, supra note 17, at 11.
84 Navias, supra note 81, at 61.
87 Navias, supra note 81, at 68.
88 Douglas Farah, Al Qaeda’s Finances Ample, Say Probers; Worldwide Failure to Enforce Sanctions Cited, WASH. POST, Dec. 14, 2003, at A01 (quoting Juan C. Zarate, the Treasury Department’s deputy assistant secretary for terrorist finance).
the Mafia,” says Richard K. Johnson, former specialist in money-laundering
and terrorist financing at IMF, “where it takes five years to get insiders.”

There is a saying that “dirty money is best passed through clean
hands.” Terrorist groups understand the truth of this statement. 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 while still circulating
millions of dollars around the world. Lawmakers and law enforcement face
the challenge of balancing the interests of many legitimate users of shell
companies with the need to cut off terrorists’ funding and the violence such
funding helps finance.

B. Defunding Terrorism: Domestic Efforts

This Part will describe both domestic and international efforts used to
combat terrorism since September 11th. The first section focuses on the
United States’ intelligence and financial efforts; the second section then
examines international intelligence and financial efforts. Finally, it
compares the overall domestic and international efforts and discusses the
shortcomings in the current environment—particularly in the private
sector—to curb the rise in the use of shell companies.

1. United States 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 and keep the borders safe. Many of these efforts, of course, focus
on domestic security—the Department of Homeland Security (DHS) and its companion agencies like the Transportation Security Administration.

---

89 Jerry Markon, Muslim Anger Burns Over Lingering Probe of Charities, WASH. POST, Oct. 11, 2006, at B01.
92 The Department of Homeland security now controls a host of functions within sub-agencies, including the Transportation Security Administration (TSA), which was created
were quickly formed to bring together law enforcement and intelligence agencies to collaboratively combat terrorism. DHS was charged with the broad mandate of “(A) prevent[ing] terrorist attacks within the United States; (B) reduc[ing] the vulnerability of the United States to terrorism; [and] (C) minimiz[ing] the damage, and assist[ing] in the recovery, from terrorist attacks that do occur within the United States.”93 With this reaching authority, many fear DHS wields too much power.94

The United States’ efforts of course also reached outside the United States—and the Department of Defense (DOD) and Department of Justice (DOJ) quickly evolved to deal with emerging international conflicts and new legal questions. Specifically, the DOD shifted its focus to preventing acts of terror rather than responding to them and increased its involvement domestically in the incapacitation of potential terrorists.95 Also, instead of only taking military action against state sponsors of terrorism,96 the DOD exercised its military force in countries that harbored terrorists within their borders.97 It has also taken part in detaining and interrogating terrorists within the United States—a practice which has been particularly controversial as of late and has caused “institutional competition” between the DOD and the DOJ.98

in the immediate aftermath of 9/11 to oversee all transportation-related security activities, with a particular focus on airport security. The Aviation and Transportation Security Act, 49 U.S.C.A. § 114 (2009).

94 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, 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 since the President was given full appointment power over five of the twenty-seven upper level DHS officials. Thessin, supra at 529–30.
95 Robert M. Chesney, The Sleeper Scenario: Terrorism-Support Laws and the Demands of Prevention, 42 HARV. J. ON LEGIS. 1, 21–22 (2005) (arguing that the DOD played a limited traditional military role in counter-terrorism efforts before 9/11 and, after 9/11, this paradigm shifted to a preventative and increasingly domestic role).
96 Id. at 22.
97 Id. at 22–23.
98 Id. at 24. This new military involvement in detaining people caught in the United States has caused a lot of controversy, particularly in concerns to one case where the detainee involved was an American citizen, Jose Padilla. Id. Although many thought that the Padilla case, which ended up going to the Supreme Court twice, would resolve the issue of military detention of potential terrorists within the U.S., in both cases the Supreme Court did not reach that question. See id.; Hanft v. Padilla, 546 U.S. 1084 (2006).
The DOJ soon expanded its authority by taking measures such as relying on the “material witness” statutes to detain suspected terrorists who otherwise could not be held. The DOJ also detained individuals based on a statute that criminalizes providing any type of “material support” to terrorists. These material support statutes quickly formed the foundation of the U.S. government’s war on terror and the key “weapon” in prosecuting terrorism domestically. These statutes have become central to the United States’ efforts in preventing terrorist financing, because facilitating such financing gives “material support” to terrorist networks. Lastly, lawmakers strengthened the capability of U.S. intelligence agencies to gather intelligence both domestically and abroad. Three important developments made this happen: (1) Congress passed the Patriot Act to amend the Foreign Intelligence Surveillance Act of 1978 (FISA), the

99 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). After 9/11, the DOJ was determined to use “every available law enforcement tool” to prevent another terrorist attack. Id (internal quotation marks omitted). Consequently, previously unenforced immigration violations became the justification for numerous arrests; however, in order to detain American citizens, the DOJ began to rely on the federal material witness statute. Id. See also Viet D. Dinh, 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 among other tools to prevent terrorist attacks); 18 U.S.C. § 3144 (2006) (material witness statute).

100 18 U.S.C. §§ 2339A, 2339B; 18 U.S.C. §§ 2339C is also a material support statute but it is rarely used. These provisions were originally passed in 1996, though very little use was made of them until after 9/11. Chesney, supra note 95, at 18–19 (“Notwithstanding the effort it took to establish [18 U.S.C. 2339A and 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.”); see also Andrew Peterson, Addressing Tomorrow’s Terrorists, 2 J. NAT’L SEC. L. & POL’Y 297, 298 (2008) (criticizing Congress for taking few steps to increase the number of criminal convictions of terrorists aside from just “build[ing] on the material support-based system that it put in place in the mid-1990’s”).


102 See Part II.B.2 (discussing the use of these statutes in greater detail).

National Security Agency implemented the “Terrorist Surveillance Program,” and (3) Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004. As a result of each of these efforts, intelligence officials can more easily prevent communication between terrorists, gather intelligence internationally and domestically, and of permissible information sharing to include state and local law enforcement personnel; 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.A. § 1805(c)(2)(B) (2005) (allowed surveillance of a person in varying areas and using different communications facilities on one order rather than requiring separate orders for each facility as before); 50 U.S.C.A. § 1861(a)(1) (expanded FBI’s ability to apply for an order for production of “tangible things” in investigations); Dinh &. Keefer, supra, 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.”).

http://www.nybooks.com/articles/18650 (letter by various legal scholars to Congress arguing that the TSP is illegal under existing law). To quell criticism. Attorney General Alberto R. Gonzales sent a letter to the Senate Judiciary Committee informing them that “any electronic surveillance that was occurring as part of the [TSP] will now be conducted subject to the approval of the Foreign Intelligence Surveillance Court.” Letter from Alberto R. Gonzales, Attorney Gen., to Patrick Leahy and Arlen Specter, Senate Judiciary Chairmen (January 17, 2007), available at


http://www.justice.gov/olp/pdf/patriot_report_from_the_field0704.pdf (outlining the
centralize recommendations and directives to the President and his advisors.  

2. United States Financial Efforts

The United States has also taken significant steps to combat terrorism financing, although its efforts in this regard are not as extensive as its military, security, and intelligence actions. In fact, the United States has come under heavy criticism for its lax regulatory scheme, for harboring shell companies, and for its non-compliance with accepted international identity requirements. U.S. Senator 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.” This is not to say that the United States has not taken any efforts to prevent terrorism financing. For example, to combat the tide of terrorism financing through charities and trusts, the Department of the Treasury gives “terrorist designations” to deprive these groups of access to illicit funds, pursuant to an executive order.

Also, to restrict the illicit use of shell companies for terrorist financing, the United States has occasionally enforced the “material support” statutes. It has also worked to specifically identify “foreign terrorist
organizations” (FTOs) and block their funding domestically and abroad.\textsuperscript{113} Regulations like these have caused pushback because of the danger of a “false positive” identification as a FTO. Notwithstanding, the United States has made significant efforts through the Patriot Act and the Money Laundering Control Act to restrict certain transactions and regulate money laundering generally.\textsuperscript{114} 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.\textsuperscript{115} Much of this was accomplished by amending the Bank Secrecy Act.\textsuperscript{116} Financial institutions

\textsuperscript{113} Section 216 of the Immigration and Nationality Act authorizes the Secretary of State to designate a group as a 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 (2004); 18 U.S.C. § 2339B (“the 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 the International Emergency Economic Powers Act. See Chesney, supra note 95, at 20.


\textsuperscript{115} Sorcher, supra note 114, at 398–99. SARs must be filed when “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,” (citing Financial Crimes Enforcement Network (FinCEN), 66 Fed. Reg. 67,670 (to be codified at 31 C.F.R. pt. 103 (2001))).

\textsuperscript{116} Enacted by Congress in 1970, and subsequently amended multiple times, the Bank Secrecy Act (BSA) “is based on the assumption that that it is easiest for law enforcement to
are also required to do more to verify the identity of their customers through “Customer Identification Programs” (CIPs), due diligence, and cross-border information sharing.\textsuperscript{117} The Patriot Act also better regulates IVT Systems,\textsuperscript{118} which, as discussed above, are utilized heavily in the Middle East and Asia to launder money through currency exchanges.\textsuperscript{119} To control other methods of money laundering, the United States has relied on the Money Laundering Control Act, which was enacted in 1998, to enforce reporting requirements and to regulate foreign money laundering through U.S. banking institutions.\textsuperscript{120}

---

\textsuperscript{117} Sorcher, supra note 114, at 400–03 (Concerning CIPs, Sorcher noted that “[f]irms are required, at a minimum, to obtain the following information 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.”).

\textsuperscript{118} To do so, the Patriot Act amends the definition of “financial institution” to include 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 the conventional financial institution system.” 31 U.S.C.A. § 5312(a)(2)(R) (2005); Shetterly, supra note 60, at 344. This is significant because it is estimated that billions of dollars cross through Pakistan and other Arab nations’ borders annually through “hawala” (an informal value transfer system) each year. Id. at 344–45 (“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.”).

\textsuperscript{119} See supra note 44 and accompanying text.

\textsuperscript{120} Under the MLCA, “it is unlawful to intentionally promote…[the] avoidance of reporting requirements, usually referred to as ‘smurfing.’” Barbot, supra note 39, at 162 (citing 18 U.S.C. § 1957 (a)(3) (2006)). This refers to making “a deposit in an amount slightly less than $10,000” in order to avoid a CTR being filed. Id. (citing Duncan E. Alford, Anti-
More recently, Senator Carl Levin has pushed to enact the Incorporation Transparency and Law Enforcement Assistance Act (ITLEA) to expose the beneficial owners of shell companies.\textsuperscript{121} It has been reintroduced with bipartisan support as well.\textsuperscript{122} While various business groups support the bill,\textsuperscript{123} it also faces significant criticism because it relies only on voluntary reporting and does not offer significant incentives or penalties for non-reporting.\textsuperscript{124} It conditions state anti-terrorism funding on an additional identity reporting requirement,\textsuperscript{125} but it does not penalize states for declining to report. Because of the loopholes that exist in the current regulatory framework, United States firms and incorporation services are required to collect only a minimal amount of identity information. Surprisingly, \textit{international} identity reporting requirements are more stringent and have been universally adopted, as discussed below.

\textbf{C. Defunding Terrorism: International Efforts}

The fight against terrorist financing requires international collaboration not only among nations but internally between government agencies and private firms.\textsuperscript{126} Though the United States’ internal efforts in many respects


\textsuperscript{121} See Carr & Grow, \textit{supra} note 70.


\textsuperscript{124} See Verret, \textit{supra} note 18, at 858, 861.


\textsuperscript{126} It essentially requires “reconceptualizing the public good of open financial systems as having negative security externalities that must be collectively managed.” Clunan, \textit{supra} note 57, at 570.
fall short, there has been a significant push internationally to stop terrorism financing through money laundering, charities, trusts, and anonymous shell companies. Foremost among those efforts has been the creation of, and recommendations issued by, the Financial Action Task Force—an intergovernmental organization working to combat money laundering and terrorism financing.\textsuperscript{127} It was established by the G-7 summit in Paris in 1989 and has grown to include thirty-six member countries, each of which provides experts to serve on the body’s governing panel.\textsuperscript{128}

Though the FATF’s recommendations are not legally binding on its members, it does require member self-assessments and “black-list” countries that are non-cooperative because they do not devote sufficient resources to combat money laundering or because their regulatory scheme is not effective.\textsuperscript{129} In addition, FATF-compliant countries threaten countermeasures against money from countries that do not solve problems within one year.\textsuperscript{130} Also, the United Nations has implemented many of the FATF’s set of “Forty Recommendations” to prevent money laundering and terrorism financing.\textsuperscript{131}

In addition to the FATF’s efforts at curbing terrorism financing and money laundering, the United Nations has taken steps as well. For example, the United Nations Security Council (UNSC) has given terrorist designations to Pakistani trusts for providing financial support to terrorism and supporting bombing efforts in India.\textsuperscript{132} In fact, in 1999—prior to the 9/11 Attacks, the UN General Assembly adopted the International

\begin{itemize}
\item \textsuperscript{127} Sorcher, \textit{supra} note 114, at 404.
\item \textsuperscript{128} FATF, FATF MEMBERS AND OBSERVERS, available at \url{http://www.fatf-gafi.org/pages/aboutus/membersandobservers/}.
\item \textsuperscript{129} Bachus, \textit{supra} note 38, at 852 (citing FIN. ACTION TASK FORCE ON MONEY LAUNDERING, NON-COOPERATIVE COUNTRIES AND TERRITORIES, available at \url{http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdicctions/}).
\item \textsuperscript{130} Id.
\item \textsuperscript{131} Sorcher, \textit{supra} note 114, at 411. In addition, following September 11, the FATF made special recommendations encouraging states to “[i]mplement UN resolutions relating to terrorist financing; criminalize the financing of terrorism, terrorist acts, and terrorist organizations; freeze funds or other assets of terrorists; require financial institutions and other businesses to report any suspicious activity where it appears that funds are connected to terrorist activities; and ensure that entities, especially non-profit organizations and charities, cannot be misused to finance terrorism.” Id. at 406 (citing FIN. ACTION TASK FORCE ON MONEY LAUNDERING, ANNUAL REPORT, available at \url{http://www.fatf-gafi.org/media/fatf/documents/brochuresannualreports/FATF%20annual%20report%202011%202012%20website.pdf}).
\item \textsuperscript{132} Nature of the Threat of Terrorist Abuse, \textit{supra} note 62.
\end{itemize}
Convention for Suppression of Financing of Terrorism.\textsuperscript{133} This Convention criminalizes knowingly collecting funds to use in terrorist activities, implements many of the FATF’s Forty Recommendations, and encourages financial institutions to report suspicious transactions.\textsuperscript{134} A mere seventeen days after 9/11, the UNSC also adopted Resolution 1373,\textsuperscript{135} a true centerpiece in the international effort to fight terrorism because of its requirement for states to criminalize the financing of terrorism and for its creation of a committee to oversee the implementation of the resolution.\textsuperscript{136} The UN has also adopted a number of other resolutions aimed at fighting terrorism financing.\textsuperscript{137}

The European Union has also made significant efforts to adopt the FATF’s recommendations. Its first directive (91/308/EEC), in fact, closely follows the FATF’s Forty Recommendations and requires member states to identify customers, keep more thorough records, and report any suspicious transactions.\textsuperscript{138} The Directive is binding on all EU members and can be enforced through legal proceedings.\textsuperscript{139} In 2004, the Directive was updated,

\begin{itemize}
  \item International Convention for the Suppression of Financing of Terrorism, UNGA 54/109 (Dec. 9, 1999).
  \item Sorcher, \textit{supra} note 114, at 411.
  \item Press Release, United Nations Security Council, Security Council Unanimously Adopts Wide-Ranging Anti-Terrorism Resolution; Calls for Suppressing Financing, Improving International Cooperation (2001); \textit{see also} Zagris, \textit{supra} note 50, at 75–76 (citing S.C. Res. 1368, U.N. SCOR, 56th Sess., 4370th mtg. ¶ 3, U.N. S/RES/1368 (2001) (This Resolution makes it imperative for 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 fund 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 measure of assistance in criminal investigations involving terrorism, and (7) prevent the movement of terrorist or terrorist groups by effective border controls and control over travel documentation)).
  \item Gardella, \textit{supra} note 50, at 125.
  \item For example, the UN Convention Against Transnational Organized Crime, “was the first legally binding multilateral treaty specifically aimed at transnational organized crime.” Sorcher, \textit{supra} note 114, at 411. Also, the UN’s Office for Drug Control and Crime Prevention (ODCCP) assists “member nations with assistance in complying with international anti-money laundering standards.” Bachus, \textit{supra} note 38, at 856 (citing \textsc{Bureau for \textsc{Int’l} \textsc{Narcotics and Law Enforcement}, U.S. \textsc{Dep’t of \textsc{State}}, \textsc{International \textsc{Narcotics Control Strategy Report}, XII-52, (2002), available at http://www.state.gov/documents/organization/8703.pdf. For a review of several other UN initiatives, see Lacey & George, \textit{supra} note 116, at 332–35.
  \item Sorcher, \textit{supra} note 114, at 408.
\end{itemize}
due in part to 9/11, to require even greater client verification procedures.\textsuperscript{140} Because the problem of terrorism financing reaches outside the standard financial and banking institutions, the EU has also expanded “gatekeeper” standards\textsuperscript{141} to include lawyers, accountants and real estate agents.\textsuperscript{142} The American Bar Association (ABA) has even created its own Task Force on Gatekeeper Regulation and Profession in 2002 to monitor compliance with these standards.\textsuperscript{143}

\textbf{D. Remaining Global Challenges}

Despite the complex domestic and international framework that has emerged since 9/11, and despite the enormous sums spent by the United States and the international community on policing terrorism financing, major gaps still exist. This is particularly so as terrorist groups now have greater access to funding through virtual channels, such as the Internet.\textsuperscript{144} First, lax domestic policies and federalism challenges—including within the United States—encourage the formation of anonymous shell companies.\textsuperscript{145} 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.\textsuperscript{146} 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.”\textsuperscript{147}

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{140} Id.
\item \textsuperscript{141} These “gatekeeper” standards actually originated at the G-8 summit, and have since been endorsed by the EU, UN, FATF, the US (through the Patriot Act), and a host of other nations. \textit{Id.} at 32–38, 46–50.
\item \textsuperscript{142} See Gregory, \textit{supra} note 56 (citing \textit{FIN. ACTION TASK FORCE, REVIEW OF THE FATF FORTY RECOMMENDATIONS CONSULTATION PAPER 98, \S 277}).
\item \textsuperscript{144} Stephen I. Landman, \textit{Funding Bin Laden’s Avatar: A Proposal for the Regulation of Virtual Hawalas}, 35 WM. MITCHELL L. REV. 5159, 5180–83 (2009).
\item \textsuperscript{145} See Browning, \textit{supra} note 74 (“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.”).
\item \textsuperscript{146} \textit{Id.}
\end{enumerate}
\end{footnotesize}
purportedly requires the least amount of information than any other state, and its approach to incorporation and LLC formation attracts companies from around the U.S. and the world.

Although the federal government—most recently through Senator Levin’s sponsorship of the ITLEA—wishes to impose more thorough reporting requirements, federalism issues present another obstacle to their implementation. For example, when the FATF published a report on U.S. compliance with its recommendations, it specifically noted a failure to designate non-compliance with certain reporting requirements as offenses under U.S. law. Some of this may stem from the anti-commandeering doctrine set forth in Printz v. United States, which prevents Congress from forcing state and local governments to implement federal programs. Although Congress made it clear in the Patriot Act that its national strategy must address enhanced federal-state cooperation, it often lacks the ability and resources to incentivize state compliance. And there is evidence to suggest that states would not voluntarily comply when the federal prerogatives run counter to state priorities. Even the FATF made note

---

148 Id. (quoting David Finzer, chief executive of a registration agent that sets up account for non-U.S. citizens).
149 Verret, supra note 18, at 892–95 (discussing the conflict between Delaware’s laws and the Incorporation Transparency Act).
150 FATF, SUMMARY, supra note 109. Among its many recommendations, the report states that “[t]here remains a gap between the policy level and operational level law enforcement work.” Id. at 15. Also, “More refined coordination is needed amongst law enforcement agencies with overlapping jurisdictions,” and “Monitoring of compliance by … the state-regulated industries is problematic, and will require further efforts.” Id. at 3.
153 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). There are others who interpret the Constitution as giving the federal government the power to force state and local governments to implement anti-terrorism programs despite the anti-commandeering doctrine. Jason Mazzone, The Security Constitution, 53 UCLA L. REV. 29, 35 (2005-2006). Professor Mazzone, for example, notes that Article IV, Section 4 of the U.S. Constitution states that the federal government has an obligation to “protect the states from invasion and domestic violence.” Id. at 35–36. The generation that ratified this clause went through the same problems the War on Terror presents today: “Security presents 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. Under Article IV, Section 4, “[T]he national government may enlist the assistance of state and local personnel as long as Congress pays the costs of their efforts.” Id.
154 See Susan N. Herman, David G. Trager Public Policy Symposium: Our New Federalism? National Authority and Local Autonomy in the War on Terror, 69 BROOK. L.
that the United States was in need of more effective internal cooperation.\textsuperscript{155} Thus, state jurisdiction over forming of corporations and other important financial mechanisms is an aspect of federalism that hinders a united domestic response against terrorism.

Second, the current and suggested framework may be at odds with concerns for business privacy and due process. First, U.S. and international policies regarding client identity and suspicious activity reporting remain controversial, often because the attorney-client privilege could be compromised.\textsuperscript{156} There are a number of recommendations to counterbalance privacy concerns, including the use of “formal nominees” in identity reporting requirements.\textsuperscript{157} Still, there is pushback from the private sector in many respects, and balancing a client’s privacy with combatting financial crime will most likely continue to be a difficult task in the future. The current regulatory framework has also been attacked on First Amendment grounds by individuals and corporations who seek to donate and transfer money anonymously.\textsuperscript{158}

Another private sector concern here is due process as assets are frozen under arguably overbroad executive powers.\textsuperscript{159} As prosecutions are carried out under the president’s executive IEEPA powers, individual litigants have tried to, though so far unsuccessfully, challenge the freezing of their assets under due process grounds.\textsuperscript{160} Additionally, the president’s statutory authority has been attacked as overbroad, since the executive power to make terrorist designations (as discussed previously) is sweeping and quasi-judicial.\textsuperscript{161} These and other concerns have stalled progress in Congress as

\textsuperscript{155} FATF, SUMMARY, supra note 109.

\textsuperscript{156} See id. at 50; see also Marc Loewenthal, \textit{Financial Privacy Laws in Conflict}, PAC. RESEARCH INST. (Aug. 8, 2002), http://www.pacificresearch.org/publications/financial-privacy-laws-in-conflict

\textsuperscript{157} PUPPET MASTERS, supra note 18, at 59–60.

\textsuperscript{158} See Buckley v. Valeo, 424 U.S. 1, 16 (1976); Guiora & Field, supra note 38 (describing the problem of money laundering, particularly through IVTS, to fund terrorism, and contrasting such illegitimate uses with legitimate religious uses for charitable and religious purposes).


\textsuperscript{160} See People’s Mojahedin Org. of Iran v. U.S. Dep’n of State, 327 F.3d 1238, 1240–41 (D.C. Cir. 2003).

\textsuperscript{161} Global Relief Found., Inc. v. O’Neill, 315 F.3d 748, 754 (7th Cir. 2002). For a more detailed explanation of the problems in this realm, see Chakravarty, supra note 159, at 308–11.
legislators attempt to strengthen the current regulatory framework. What, if anything, within the aforementioned statutory and regulatory framework is influential at stopping the flow of terror financing? Are international or domestic regulations more effective? These questions and others are addressed in our experiment, below. The study that follows identifies which countries and institutions comply less frequently with identity reporting requirements and what factors might influence whether an institution agrees to help form a shell company.

II. EXPERIMENTAL RESULTS

In an effort to mount a war on terror the United States has taken bold steps—both domestically, as well as internationally—to safeguard its interests and to protect its borders. It has strengthened the military, expanded the scope of its intelligence-gathering efforts, and increased law enforcement powers under the Patriot Act. The United States has spent billions to combat terrorism around the world.

But while these efforts have done much to disrupt and dismantle terrorist networks worldwide, security officials and commentators are concerned that the United States has not invested sufficient resources to cut off the true terrorist lifeline: illicit terrorist financing. 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 in Part II, terrorist organizations launder money through trusts, charities, and shell corporations.

The international community—particularly through FATF recommendations—has responded by developing policies to combat money laundering and terrorism financing. IGOs and nations such as the United States simultaneously enacted extensive regulations that track the FATF

---

162 See Part II.C.1
163 See Part II.C.2
164 See Part II.C.3
165 See footnotes 4–8 and accompanying text.
166 PERL, COMBATTING TERRORISM, supra note 10.
168 See Part II.A
recommendations. These efforts produced strict regulation governing the formation of shell companies, and the “anonymous” shell corporation was—at least on paper—completely prohibited.

While these international and domestic laws have been in place for years, no empirical studies have been conducted to investigate their effectiveness. Previous articles have been written which attempt to show how easy it is to form a shell company, but they have only provided a few anecdotal examples or, at most, a summary of several examples of shell companies. By contrast, our study used 7,466 approaches for 3,773 providers in 182 countries. What also sets this study apart is that it uses a variety of approaches to determine what factors make providers more or less likely to comply with domestic and international regulations affecting the formation of shell companies.

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. In answering this question, we first seek to discover which countries are the most compliant and what factors might contribute, in contrast, to non-compliance. We then gauge the effectiveness of U.S. domestic regulations to discover whether compliance by U.S. firms/incorporation services differs in any respect from the international community. Finally, we compare the results from both the international and domestic tests and analyze what contributing factors make some countries more or less compliant than others.

A. Design Study: Finding Providers, Composing Treatments

In determining the effectiveness of post-9/11 financial regulations, we focus our analysis on countries’ informal compliance with FATF recommendations and IRS regulations by way of private actors, including firms and incorporation service providers. Mindful that the field

170 For example, the USA PATRIOT Act, the Foreign Account Tax Compliance Act, and the International Emergency Economic Powers Act.
172 See sources listed in supra note 25.
173 For a more thorough analysis of formal compliance, see Baradaran et al., Does International Law Matter?, MINN. L. REV (forthcoming). Formal compliance is easier to gauge because it is seen in the steps the nation takes to implement and enforce international
experiment is occasionally criticized because it contributes only a pragmatic, “what works” analysis, we focused on the larger theoretical questions. Accordingly, this field experiment presents more than statistics. Instead, we utilize the major international law and relations theories to get to the heart of what actually causes compliance.

To complete this experiment, we first had to compile a list of incorporation services providers and, second, create a pool of e-mails sent from a number of aliases we created to pose as international consultants seeking an anonymous shell corporation. First, to find a compile the list of providers, we were tasked with performing Google searches for terms such as “company formation” and “business law” because no definitive list exists of incorporation service providers. We were successful in collecting a pool of 3,773 corporations and law firms drawn from nearly every nation of the world—182 to be precise. 1,785 of these were from the United States, 444 from other OECD countries, 1,039 from developing nations, and 505 from countries with reputations as tax havens. This does not, of course, represent every incorporation services provider, but its 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 2,051 firms that included 63 US firms and all of the other non-US firms. In the second, the remaining 1,722 US firms were subjected to the same FATF conditions, but were also presented with additional conditions, including a treatment to test the effectiveness of IRS regulations on each of the providers. All of these conditions will be explained below.

Next, to complete each of these experiments, we sent emails that were treated with different experimental conditions. Before discussing how these treatments differed, we first note that each e-mail 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 (ranging from reduced liability to 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 transparency law. See Brummer, supra note 169, at 291. This, however, is not the focus of this study.

174 Susan D. Hyde, The Future of Field Experiments in International Relations, 628 THE ANN. OF AM. ACAD. POL’T. & SOC. SCI. 72, 75 (2010) (noting that field experiments are often criticized for failing to address big questions and only dealing with insignificant phenomena).

175 See infra note 193 for a discussion of managerialism and its intersection with this study.
domestic regulation. The firm is then able to decide to either comply or refuse to comply with transparency standards. The emails allegedly originate from various areas of the world ranging from low-corruption Organization for Economic Cooperation and Development (OECD) nations,\(^\text{176}\) to nations that are generally associated with terrorism.

1. Placebo

The first e-mail was our “placebo” or control,\(^\text{177}\) which was sent from one of eight smaller, wealthier countries, less perceived as “corrupt” or at risk for terrorist influence. The placebo is the only treatment that does not specifically reference an element of international or domestic law. It is also the least suspicious of the emails for a couple of reasons. First, the placebo email hails from relatively wealthy, low-corruption OECD countries. These are Denmark, New Zealand, Finland, Sweden, Netherlands, Australia, Norway, and Australia. For convenience, they are collectively referred to as “Norstralia.” Each nation in the Norstralia group is listed as among the least corrupt countries on Transparency International’s Corruption Perceptions Index (CPI).\(^\text{178}\) Additionally, to ensure against the potential for national or regional bias, we varied the name and location of the consultants. Therefore, other than asking for anonymous incorporation, the placebo email does not contain anything especially suspicious. Where the e-mail hailed from a non-English speaking nation, we injected two spelling, syntax, or grammar errors to enhance their authenticity. This control e-mail served as a benchmark to compare to the rest of the responses in both response rates and requests for identity documentation.

Including the placebo e-mail, we used 12 different treatments, which are summarized in Table 1. All of the treatments are summarized in Table 1, below, and we discuss the first eight in detail in subsequent sections.

\(^{176}\) The Organization for Economic Cooperation and Development (OECD) includes twenty countries including these listed in the text along with relatively wealthy countries such as the United States and the United Kingdom. See OECD, MEMBER COUNTRIES, at http://www.oecd.org/countrieslist/0,3351,en_33873108_33844430_1_1_1_1_1,00.html.

\(^{177}\) See Appendix A (Placebo E-mail)

\(^{178}\) Other top ten CPI countries, such as Switzerland and Singapore have been excluded because they are associated with financial secrecy or other “tax-haven” conditions. Interviews and other material from the corporate sector indicate that the prospective client’s country of residence and the business sector are the primary indicators of risk to the finance industry. KPMG INT’L, GLOBAL ANTI-MONEY LAUNDERING SURVEY 25 (2007).
Table 1: Summary of Treatments

<table>
<thead>
<tr>
<th>Condition</th>
<th>Key Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Placebo</td>
<td>Alias originates from low-corruption, minor-power “Norstralia” country.</td>
</tr>
<tr>
<td>Corruption</td>
<td>Alias hails from high-corruption “Guineastan” country and works in government procurement.</td>
</tr>
<tr>
<td>Terrorism</td>
<td>Alias claims citizenship in one of four nations associated with terrorism and purports to work in Saudi Arabia for an Islamic charity.</td>
</tr>
<tr>
<td>FATF</td>
<td>Alias notes that the Financial Action Task Force requires identification.</td>
</tr>
<tr>
<td>Penalties</td>
<td>Alias notes FATF standards and invokes the possibility of legal penalties (for international firms only).</td>
</tr>
<tr>
<td>IRS</td>
<td>Alias notes that the Internal Revenue Service enforces disclosure requirements (for U.S. firms only).</td>
</tr>
<tr>
<td>Premium</td>
<td>Alias offers to “pay a premium” to maintain confidentiality (for international firms only).</td>
</tr>
<tr>
<td>U.S. Origin</td>
<td>Alias originates from the United States (for international firms only).</td>
</tr>
<tr>
<td>Norms</td>
<td>Alias notes FATF standards and appeals to international norms (intn’l firms).</td>
</tr>
<tr>
<td>ACAMS</td>
<td>Alias attributes identity rule to private Association of Certified Anti-Money Laundering Specialists (intn’l firms).</td>
</tr>
<tr>
<td>ACAMS+FATF</td>
<td>Alias attributes identity rule to both ACAMS and the FATF (intn’l firms).</td>
</tr>
<tr>
<td>No Documents</td>
<td>Alias does not mention identity documents (intn’l firms).</td>
</tr>
</tbody>
</table>

2. Corruption Treatment

The next email is slightly more suspicious. In this treatment, we send out emails that purportedly originate from countries that are seen as high-risk in crime and terrorism according to the Transparency International’s Corruption Perceptions Index (CPI). These are Guinea, Guinea Bissau, Equatorial Guinea, Papua New Guinea, Kyrgyzstan, Tajikistan, Turkmenistan, and Uzbekistan. We refer to these collectively as “Guineastan.” This treatment tests the effectiveness of the FATF’s

---

179 See Appendix A (Corruption Treatment)
36

injunction against those nations “identified by credible sources as having significant levels of corruption, or other criminal activity.’’ To raise the risk of corruption from these countries, the consultants posing in each of these emails claimed to work in procurement for each country’s government, one of the most notoriously corruption-prone industries. Collectively, each of these factors should have made the corruption motive quite apparent.

3. Terrorism Treatment

In this third treatment, we pose as terrorist risks. We attempt to create an Islamic charity and hail from countries recognized as sites of suicide terror: Lebanon, Pakistan, Palestine, and Yemen. In this treatment we test the effectiveness of two of the FATF’s standards. First, the FATF’s warning against “[c]ountries identified by credible sources as providing funding or support for terrorist activities that have designated terrorist organizations operating within them.” And second, the FATF requirement that companies screen “charities and other ‘not for profit’ organizations which are not subject to monitoring or supervision.” The combination of (1) individuals from a country perceived as a host to terrorists, (2) working for an Islamic charity, and (3) seeking financial secrecy presents a very unsubtle terrorist financing risk.

4. FATF, Penalties, and IRS Treatments

Our FATF treatment adds to the basic control template. It purportedly originates from one of the eight “Nostralia” countries listed above and the consultant directly references FATF provisions that require the production of identification to create a shell corporation. This treatment contains the most straightforward reference to FATF. After referencing the provisions,

\[\text{\footnotesize 181} \text{ FATF, RBA GUIDANCE FOR TRUST AND COMPANIES SERVICE PROVIDERS (TCSPs) 21 (June 17, 2008), http://www.fatf-gafi.org/media/fatf/documents/reports/RBA\%20for\%20TCSPs.pdf [hereinafter FATF, RBA GUIDANCE]}\]

\[\text{\footnotesize 182} \text{ See Appendix A (Terrorism Treatment)}\]

\[\text{\footnotesize 183} \text{ ROBERT PAPE, DYING TO WIN (Random House 2005).}\]

\[\text{\footnotesize 184} \text{ FATF, RBA GUIDANCE, supra note 181, at 21.}\]

\[\text{\footnotesize 185} \text{ Id. at 22.}\]

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, and legalization. These theories suggest that noncompliance is the direct result of either ignorance of the law, or ignorance of the conditions in which the law should be applied. Therefore, we would expect to see high numbers of compliance because the international law email explains not only the law, but also the specific context in which it should be applied.

The next two treatments—the Penalties and IRS treatments—add the same information as the FATF standard, but they also mention the possibility of either FATF or IRS sanctions in the case of non-compliance. Even though the IRS does not have identity reporting requirements, we included this information to see if it would act as an additional deterrent. Our expectation was that including all of this additional information would raise the proportion of complaint countries and/or lower the number of providers willing to do business.

5. Premium Treatment

In the fifth treatment, we offered to pay a premium to preserve confidentiality. This treatment is used to determine the effectiveness of the FATF’s requirement that corporations screen potential clients who offer “to pay extraordinary fees for services which would not ordinarily warrant such a premium.” The question here was whether the effect would lower response rates and increase compliance rates or if CSPs would be enticed by the additional premium.

All of the above described email treatments were sent from accounts registered to mobile phone numbers purchased in an African country and sent by researchers in the United States, but masked through a proxy server to make it appear as though they were sent from various countries in East Asia and Europe. If the CSP did not respond within a week, a follow-up was sent. If the CSP was asked about identity documents and did not reply on that issue, they were sent a follow-up email to request the information again.

---


189 FATF, RBA GUIDANCE, supra note 181, at 22.
B. Coding the Responses

1. Compliance Coding

After forming the treatments and sending out e-mails according to the aforementioned protocol, we were tasked with appropriately coding the responses to effectively measure our results. We coded five responses in furtherance of this result: (1) no response, (2) non-compliant, (3) partially compliant, (4) compliant, and (5) refusal.

CSPs who decided not to respond may not have responded for a number of reasons. It could be risk avoidance (discussed later in the results section), or it could be for purely commercial reasons, an excessive workload, or a judgment that aiding the customer involved significant risk. Some responses recognized the email as a scam, while others could be interpreted as seeking more information and requesting a higher premium.

To be coded as “compliant,” each CSP must have asked for specific government-issued photo identification, whether it be notarized or certified. This could include a photocopy of a passport page together with utility bills. This information is then stored by the CSP should law enforcement or regulatory officials request the documentation. The Appendix contains an example of a compliant response.

Partially compliant CSPs must have at least requested some form of identification, but fell short of the notarized copies of government-issued identity documentation. Non-compliant CSPs were those that offered to assist in forming an anonymous shell corporation without any identity documents whatsoever.

To ensure that responses were coded accurately and consistently, each response was coded twice by separate research coders in accordance with a formal manual. In the case of discrepancies, a senior research coder arbitrated the codes and assigned them a final value.

2. Random Assignments

The logic behind this experiment is to discover what factors make a CSP more or less likely to comply with international and domestic regulations regarding the formation of shell companies. The randomization of the treatments involved here helped to ensure that, like any other clinical

---

190 See Appendix B (Indignant Response)
191 See Appendix B (Response to Premium Treatment)
192 See Appendix B (Compliant Example)
193 See Appendix B (Non-Compliant Example)
trial, the other average differences would be neutralized. Like a random pool of volunteers for a medical trial, the CSPs are also randomly distributed to each of the different treatments. Because the pool of CSPs in this experiment is so large, we can be confident that extraneous factors will be balanced out between the different test groups. In this way, we can accurately measure differences against the initial control group and correctly attribute differences in compliance rates to the singular factor we have drawn out in each of the treatments.

C. Results and Findings

1. Brief Summary: An Overview of Compliance Rates

   After sending our treated e-mails and coding the responses, three key findings emerged from the study.

   First, risk of corruption was not as effective a deterrent as a risk for terrorism. In contrast to the terrorism indicator, which was the most effective treatment in our study, the corruption indicator actually decreased compliance in both the domestic and international samples when compared to the placebo.

   Second, we found that including information on international and domestic regulations had much less of an impact than anticipated. While the mention of U.S. regulations actually impacted compliance, mentioning international regulations had no measurable impact. Also, offering a premium to bypass these regulations was disconcertingly effective.

   Third, compliance between countries and U.S. states was inconsistent with any international relations theory. Compliance rates varied drastically from country to country, as well as between the individual United States, independent of the country’s wealth or level of development. States with lax financial regulations, such as Wyoming and Delaware, were the worst offenders in the sample and almost without hesitation accepted offers to assist in forming shell companies, regardless of the risks involved and the information provided. Also, countries that are notoriously known as “tax havens” were actually some of the most compliant countries in our study.

2. Complete Discussion of Findings

   We categorize our overall findings into six main sections: (1) the overall effectiveness of KYC rules requiring identity documentation both among all countries generally and then specifically among U.S. CSPs; (2) relative compliance rates among tax havens, OECD countries, and poorer developing nations; (3) the (in)sensitivity of CSPs to terrorism and
corruption risks; (4) the effects on compliance when CSPs were given more information about the rules and penalties for noncompliance, including penalties and IRS information; and (5) the relative compliance among individual states within the U.S., and challenges that might explain the disparate results.

In describing the compliance rates among 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 non-compliance offer to incorporate. Thus, if the non-compliance rate were 5 percent, the Risk Aversion Level would be 20. The lower the level, the easier it was to find non-compliant CSPs. Very high Risk Aversion Levels (meaning very low rates of non-compliance) 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 Non-response (e.g. Utah), or some combination of each of these results. So a high Risk Aversion Level could be attributed to a combination of these different patterns.

As discussed previously, basic FATF requirements mandate authorities to have “adequate, accurate, and timely information” on the real, beneficial owners of any given shell company. This rule is only truly complied with if CSPs collect fundamental identity documents, and compliance with this rule is essential to fight a range of financial crimes and combat terrorism. Yet before this study, policymakers had no data to know to what extent the rule is actually followed.  

a. Overall International Know-Your-Client Effectiveness

Our results demonstrate low rates of effectiveness of international and domestic know-your-client laws, particularly within the United States. When compliance is measured across all countries and including all treatments (the broadest level—7,466 inquiries), the non-compliance level for the international sample, including the 63 U.S. firms, is 8.4 percent with an overall Risk Aversion Level of 12. This compliance rate of 8.4 percent includes non-responses (refusals) in the denominator, since some CSPs may fail to reply—thus complying with international law in a “soft” way. In

---

194 The only information on this has been FATF audits and reports submitted to the FATF by signatories.
195 Internationally, 49.3 percent of our approaches did not reply. The ratio was even higher in the U.S. sample at 77.3 percent, and U.S.-based law firms were highest at 83 percent. What does this high level of non-responses mean for our results? This could potentially be considered “soft compliance” because a provider thought the request was too suspicious. If
contrast, within the U.S. sample, the noncompliance level is 9.2 percent and the Risk Aversion Level was 10.9—almost 10 percent lower than the international sample. This demonstrates that obtaining an anonymous shell company is actually easier in the United States than the rest of the world.

However, two factors may contribute to this wide gap. First, there is a higher non-response rate from U.S. CSPs in the sample (77.3 percent compared to 49.3 percent in the international sample). The proportion of U.S. providers who replied to our inquiries and required no identity documentation whatsoever was 41.5 percent, which is roughly two-and-a-half times the 16.5 percent average in the international sample. For those firms that failed to reply, we sent a second e-mail simply asking if the firm was still in business and assisting customers but made no mention of confidentiality, taxes, or liability. What resulted was that the vast majority of non-responsive CSPs are not soft refusals—instead, they fail to respond to any inquiry—even the most innocuous ones.

Second, there is a great disparity between U.S. business law firms and CSPs in their compliance rates (see Figure 2 below). Business law firms replied at much lower rates than other CSPs (16.6 percent in the U.S. compared with 55.5 percent of all CSPs). These other CSPs were also especially unlikely to ask for identity documentation. In fact, in general only a tiny proportion of U.S. providers actually met the more stringent international identity requirements (10 of 1,722 U.S. providers, or 0.0058). Overall, U.S. business law firms were much less likely to violate international laws that prevent the funding of terrorism.

this is generally true, it would indicate that the system works better than we generally suggest, because most of the non-responses could be judged as evidence of a functioning regulatory framework. On the other hand, if non-responses bear no relation to de facto risk screening and are merely a product of commercial decisions, uninterest or disorganization, then non-responses cannot be regarded as evidence that the system is functioning.

Our evidence suggests that the latter possibility is most likely and that most non-responses do not reflect customer risk. To test this, we sent a brief, no-risk follow-up email to all non-responsive providers, using a different Norstralia alias and asking if they were still in business and assisting customers. Among the CSPs that failed to reply to any previous email, 91 percent of the international providers and 92 percent in the U.S. did not respond to this most innocuous inquiry, indicating that customer risk had little to do with their silence.
Figure 1: Risk Aversion Level by Treatment. International and U.S. results are reported separately. Asterisks denote statistical significance: ***p<0.01; **p<0.05
b. Relative Compliance Rates Among Countries

The relative wealth of countries seems to have no impact on whether they are likely to enforce international laws that prevent the funding of terror. In our experiment, wealthy OECD countries (including the United States) were actually the worst at enforcing international identity incorporation requirements. This runs counter to the conventional wisdom that poor countries would be least compliant (see Figure 2 below). For developing countries, the Risk Aversion Level is 12 whereas in OECD countries it is 7.8 (and, with tax havens, it is 25.2, as discussed below). This finding is significant because it demonstrates that it may not be particularly expensive to enforce these identity requirements since poorer countries fare better.\(^{196}\) This may indicate that countries who fail to comply show an unwillingness to enforce the rules, rather than any kind of incapacity as some experts have posited.\(^{197}\) In fact, it is easier to obtain an untraceable shell company from a CSP (non-law firm variety) in the United States than in other country other than Kenya.

---

\(^{196}\) See Baradaran et al., supra note 173.

\(^{197}\) These findings run counter to the managerial theory, which posits that non-compliance is a result of a lack of resources and information, rather than an unwillingness to comply. Abram and Antonia Chayes, central proponents of this theory, argue that the best way to “manage” compliance, then, is to provide states with the information and resources they need, rather than the mere threat of sanctions. Chayes & Chayes, supra note 187.
Figure 2: Risk Aversion Level by Type of Country Internationally and by Provider Type in the United States
This contradicts the overwhelming consensus that tax havens provide particular secrecy and lax regulation, particularly with shell companies. This is articulated in G20 communiqués, NGOs, and is also widespread in U.S. media.\textsuperscript{198} Service providers located in tax havens, surprisingly, made it more difficult to form anonymous shell companies than OECD countries and developing nations. In fact, tax havens were more compliant than any other country group with a Risk Aversion Level of 25.2—much higher than the OECD score of 7.8. This means that it was three times more difficult to obtain 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 Bahamas, are among the most compliant in the world, while developed nations like the UK, Australia, Canada, and the United States rank near the bottom (see Figure 3). Also, it is important to note that our experiment does not consider tax havens compliant unless they make clear that they require identification information for beneficial owners of the company, which avoids the problem of these legal fictions.\textsuperscript{199}


Figure 3: Risk Aversion Level by Country for Nations with at least 25 approaches. All 25 U.S. firms from the U.S.-only sample are included together with the 63 U.S. firms in the international sample. Firms in the top eight countries were never found noncompliant. Because there is no natural upper bound on the Risk Aversion Level, we set it to 100 for these, but they should be interpreted as having a record without any noncompliance.
c. The (In)sensitivity to Terrorism and Corruption Risks

Overall, our results demonstrate a disturbing level of insensitivity to the risk of corruption. Indeed, the corruption treatment resulted in some interesting outcomes when compared to the placebo benchmark. First, there was very little difference between the relatively innocuous “Norstralian” placebo email and the high-risk “Guineastan” treatment that signals corruption even though the treatments were substantially different. In the international sample, the Risk Aversion Level was 11.5 for the Placebo, 11.3 for Guineastan, and 18.5 for the Terrorism financing risk. United States firms were even less likely to deny incorporation with a Risk Aversion Level of 9 for the Placebo, 9.9 for Guineastan, and 17.4 for Terrorism treatment (see Figure 1 above). What is most disconcerting is that the corruption risk significantly reduced compliance, despite FATF guidelines specifying that these customers should receive heightened scrutiny (see Tables 2 and 3)\textsuperscript{200}. These overall rates were reduced because both compliance rates in the international sample and refusal rates in the U.S. decreased.

By contrast, the terrorism financing results are mixed. To begin, customers shopping under this treatment were less likely to receive a reply. In fact, nearly 60 percent of requests in the international sample and over 80 percent in the domestic sample received no response, which suggests an increased number of “soft” refusals. Also, the international and U.S. results demonstrate that the Terrorism treatment causes significantly lower Non-Compliance rates compared to the placebo, which seems to suggest that potential terrorists face a more difficult task in incorporating anonymously.\textsuperscript{201} But this is offset by the fact that the Terrorism treatment also decreased the rate of Part-Compliance in the international pool, meaning firms were less likely to ask possible terrorists for at least some non-notarized I.D. form than in the Placebo condition. For instance, in the international sample, the Part-Compliant rate was only 11.6 percent, compared to 16.5 percent with the placebo. This result may indicate that the level of risk tolerated by at least a large number of firms may be higher with the Terrorism treatment than with others. And to go even further, firms that recognize the terrorism red flags, demonstrate that they actually may want

\textsuperscript{200} For a more comprehensive review of these FATF guidelines and its push for a “risk-based approach” (RBA), see FATF, RBA GUIDELINES, supra note 181.

\textsuperscript{201} The federal government has made efforts to provide information to incorporation service providers on “red flags” that indicate terrorist financing, which may have contributed to this finding. FED. FIN. INST. EXAMINATION COUNCIL, supra note 17.
to be left in the dark about the identity of the individuals they are dealing with to avoid potential liability.\footnote{In some ways, this is not surprising given the lax level of domestic regulation in many countries, including the United States. For one profound anecdotal example, see NPR, \textit{Shell Game: 2,000 Firms Based In One Simple House} (July 2, 2011), 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 service providers stand to profit greatly and they are an integral part of many economies, including the Netherlands. Crouch, supra note 69.}

In the U.S. sample, the results were much of the same. Potential terrorists received fewer refusals when compared to the international sample. However, in contrast to the international sample, since virtually zero firms were asked for supporting identification in the United States, a refusal was the only way U.S. firms complied with FATF standards, so it is particularly worrisome that the compliance rate dropped so dramatically in this sample. As a result, it was easier to form a terrorist organization in the United States than in the rest of the world.

Overall, the Corruption and Terrorism findings provide evidence that the principle of a “risk-based approach,” meaning that CSPs would be risk-adverse to customers with a Terrorism or Corruption risk, is inadequate. Though riskier customers should receive heightened scrutiny, CSPs have been ineffective at screening corrupt customers. Even customers with an obvious risk of terrorism were not required to give identifying information. As such, policymakers may reconsider a “risk-based approach” in setting domestic regulations and incorporation standards, since it may not be effective. Additional government oversight or domestic penalties may prove more effective in improving scrutiny by firms.\footnote{In the United States, there are a number of agencies tasked with providing oversight to screen for transactions that have a high potential for involvement in terrorist financing. For example, the CFTC is given authority and oversight under provisions in the Patriot Act (through amending the Bank Secrecy Act). CFTC, \textit{ANTI-MONEY Laundering}, http://www.cftc.gov/industryoversight/antimoneylaundering/index.htm.}

d. The Effect of Additional Information: IRS and Penalties

We tested three different questions in the subsequent treatments: (1) Does informing providers about the rules make them more likely to follow them? (FATF treatment); (2) Does raising the prospect of penalties make providers any more likely to comply with KYC rules? (IRS; also IRS v FATF standard); (3) Does offering more money to providers to violate the rules make them any more likely to do so? (Premium treatment) We found, in brief that, (1) information \textit{doesn’t really} induce additional CSP
compliance; (2) informing CSPs of penalties partially induces compliance; and (3) offering an additional premium for anonymity does make them more willing to violate international guidelines.

Our experiment demonstrated that informing firms about international laws requiring identity information did not increase their acting in accord with these laws. There was little difference between the benchmark Risk Aversion Level (11.5 international, 9 U.S.) and the FATF treatment (11.2 international, 10.2 U.S.). Also, the Penalties treatment did little to induce compliance (13.2 internationally), such that informing firms that they would be subject to international penalties did not foster more compliance. But the prospect of IRS enforcement significantly decreased the Non-Compliance rate in the United States, thereby boosting the Risk Aversion Level from 9.5 (Placebo) to 13.2 (IRS). These findings demonstrate two important points: (1) it is not ignorance of the law that causes global non-compliance; and (2) threat of IRS enforcement (a domestic penalty) has a greater effect than knowledge of FATF standards (an international penalty).

Concerning the premium treatment, offering providers more money to incorporate anonymously decreased the chance they would be found non-compliant, boosting the Risk Aversion Level from 11.5 to 16.6, but this increase was not statistically significant. However, there was a statistically significant decrease in the Compliance rate from 18.9 (Placebo) to 14.2 when the Premium treatment was imposed. Overall, offering firms extra money to keep identity information confidential made them more likely to break the law, if they responded to our requests.

e. Variation Among U.S. States

There was considerable variation between the individual U.S. states concerning identity requirements. Wyoming, Delaware, and Nevada were among the worst in compliance rates—a particularly worrisome finding demonstrating that providers in these states are most likely to sell companies to foreign clients (See Figure 4, below). These states, as well as Oregon, were recently cited by the U.S. Treasury’s Financial Crimes

---

204 The U.S. Treasury, together with multiple agencies including the IRS, have formed a working group to assess the threat of money laundering. Unsurprisingly, one of the working group’s reports noted that shell companies and trusts were a major area of concern in states like Delaware and Wyoming. U.S. DEP’T TREASURY, U.S. MONEY LAUNDERING THREAT ASSESSMENT 47 (Dec. 2005), http://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/mlta.pdf. It is hoped that 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 the use of SARs), that this activity will decline.
Enforcement Network (FinCEN), as being “particularly appealing” locations to form shell companies. FinCEN also noted that Delaware was the worst offender. It comes as no surprise that these states have some of the worst compliance rates because, as discussed previously, these states also have the most relaxed identity requirements for forming a shell company. A more careful analysis of the states we found to be most and least risk-averse in our study is in order.

So why do states continue to allow relaxed identity reporting requirements, despite the risks of corruption and terrorism that such a practice invites? Large profits are one answer. Cyrus R. Vance, Jr., District Attorney for Manhattan, recently explained: “Secrecy [in forming shell companies] has become a big business.” In fact, major U.S. corporations, including Exxon, Chevron, and Rio Tinto, use a number of Delaware subsidiary companies to transact business. However, there is not enough federal involvement to prevent this longstanding practice. While legislation such as the ITLEA would allow the federal government to require states to impose more thorough identity reporting requirements, it has continually been blocked in congressional committee. And while federal regulation is one way to accomplish more oversight, another way may be to compare the least and most compliant states to determine what differences these states provide as far as oversight. In particular, the states that were found to be perfectly compliant—including Arkansas, Maine, Utah and Minnesota—should also be studied to determine if any regulations propagated there induced greater compliance among their firms. At the very least, these

205 Wayne, supra note 147.
206 Id.
207 See Part II.A.3.
208 Cyrus R. Vance, Jr., Commentary: It's Time to Eliminate Anonymous Shell Companies, REUTERS (Oct. 9, 2012), http://newsandinsight.thomsonreuters.com/Legal/News/2012/10_-_October/Commentary__It_s_time_to_eliminate_anonymous_shell_companies/
209 Wayne, supra note 147.
211 While there have not been studies comparing compliance among the various states, the FATF, in its 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, THIRD MUTUAL EVALUATION REPORT, supra note 109, at 256–57. The report did note, however, that thirty-seven states, as well as the District of Colombia, have joined together with the Money Transmitter Regulators Association (MTRA) (a non-profit) to draft model legislation and regulate Money Service Businesses (MSBs). Id. at 256.

Also, the Financial Crimes Enforcement Network (FinCEN), in studying the role of shell companies among the various states, noted that while “some states require the reporting of
results will be illuminating to state policy makers interested in creating a business-friendly environment but also weary to open their doors to terrorism and corruption.

---

information on ownership, no state requires the reporting of information on beneficial ownership.” The Role of Domestic Shell Companies, supra note 17, at 3. FinCEN also found that 14 of the states with the least amount of transparency also had absolutely no requirement to report the identities of members or managers of LLCs. Id. at 9. Whether there is a more direct correlation between the stringency of state regulations and ease of forming a shell company is a topic for further study and consideration.
Figure 4: Risk Aversion Level by State in the U.S. for all states. Similar to Figure 3, firms in none of the top eleven states were found noncompliant. Because there is no natural upper bound on the Risk Aversion Level, we set it to 100 for these as well. But they should be interpreted as having a record without any noncompliance.
III. The Future of the War on Financial Terror

The results of our international global field experiment demonstrate that the U.S. goals in the war on terrorist financing have fallen well short of the mark. International and domestic laws since 9/11 have worked to increase information sharing and created restrictions on the financial sector, but many firms are still more than willing to aid in forming anonymous shell companies. This experiment challenges the efficacy of these laws by exposing the large gaps that exist.

Specifically, we tested how easy it is to form an anonymous shell company without adhering to identity requirements embedded in universally accepted international laws. The results are disturbing. International laws requiring identity of customers to form shell companies are not effective. Almost half of the companies we approached did not ask for proper identification and 22 percent did not require any identity documents at all to form a shell company.

We found that knowledge of international laws does not result in firms being more likely to require identify information in forming companies. We also found that forming an anonymous shell company—capable of funding terrorism and corruption—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 any other country besides Kenya. And within U.S. states, the worst offenders of international corporate transparency standards were Delaware, Wyoming, and Nevada, the most business-friendly states.

In combination, the above results are not good news in terms of the effectiveness of the current domestic and international regulatory framework. Shell companies are clearly widely available and easy to procure. More developed OECD countries—including the United States and others who participate directly with the FATF—are some of the worst offenders in terms of identity reporting requirements. In fact, it is three times easier to form an anonymous shell company in an OECD country than in the oft-reviled tax havens. And tax havens are the hardest places in the world to form anonymous shell companies.

Additionally, firms weren’t any less reticent to contravene international laws when we informed them about penalties that accompany international regulations. But U.S. firms were less likely to aid an individual seeking to

---

212 See Figure 3. Kenya ranks at the very bottom of all 62 countries in the relevant sample in terms of Risk Aversion; U.S. Incorporation Services, which have the second-worst Risk Aversion Level, scored only slightly better than Kenya. U.S. service providers generally (a sample which includes both U.S. law firms and incorporation service providers) still fell into the bottom third of all countries in the sample.
form an anonymous shell company when we provided them with more information regarding the IRS. In fact, mentioning that IRS regulations required disclosure—even though there is no such requirement—induced more compliance than mentioning the substantive international FATF recommendations, which had no effect at all. This empirical evidence supports incorporation of FATF recommendations—particularly more stringent identity requirements—into domestic regulation.213 Thus, our experiment does leave some hope that increased domestic regulation and enforcement of international laws could improve compliance.

Our research suggests that government must demonstrate a commitment to enforcing these regulations and work more closely with the private sector if it wishes to curb terrorism financing. Two important findings here demonstrate that this close collaboration between government and the private sector provides some hope. First, there is great variation among nations throughout the world in their compliance rates with international identity requirements, demonstrating differences in levels of commitment between governments throughout the world. The countries that are most compliant, ironically, are tax havens.214 But this finding is not as surprising


214 See Figure 3. Our findings strongly suggest that notorious tax havens like the Bahamas, Cayman Islands, and the Isle of Man are actually quite compliant in terms of requiring identity documentation. However, the FATF as recently as 2000 placed these nations on its blacklists. Peter Lilley, The FATF ’Blacklist,’ DIRTY DEALING (2006), http://www.dirtydealing.org/IMAGES/fatfblacklist/The%20FATF%20Blacklist.pdf. Furthermore, these countries still brandish a reputation as sites for money laundering, which may be partially due to political rhetoric. Daniel J. Mitchell, Tax Havens are Not Money Laundering Centers, CATO (Feb. 9, 2010: 1:00 P.M.), http://www.cato.org/blog/tax-havens-are-not-money-laundering-centers.

Other studies, as well as FATF’s most recent categorization of “high risk” jurisdictions, do not list any of these so-called “tax havens” as high-risk countries. BASEL INST. OF GOVERNANCE, Money Laundering and Terrorist Financing: High Risk Jurisdictions, available at http://baselgovernance.org/fileadmin/docs/LISTE.jpg. See also FATF, HIGH-RISK AND NON-COOPERATIVE JURISDICTIONS (Oct. 2012), available at http://www.fatf-gafi.org/topics/high-riskandnon-cooperativejurisdictions/.
as it may seem upon further examination. In tax haven countries, government regulators work very closely with private firms to enforce know-your-client regulations and other identity requirements. These governments understand the importance of business clients and want to maintain a respectable reputation internationally for incorporation and banking. With this close government oversight, despite the negative press some tax havens have received over the years, they maintain near perfect compliance in our field experiment.

By contrast, a number of U.S. states like Delaware, Nevada, and Wyoming have abysmal compliance records. The United States has not taken identity transparency seriously with any domestic enabling legislation to implement international requirements, allowing a race to the bottom with states within the U.S. willing to incorporate anyone—including, as our experiment demonstrates, high risk clients. The extremely low compliance levels of Delaware compared to those of the tax havens is most

---

This information 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 Curtis A. Ward, National Security, Terrorism and Smuggling (Dec. 17, 2010), http://www.caribbeanresearchandpolicycenter.org/publications/docs/ (discussing current efforts by officials in the Cayman Islands). For example, officials in the British Virgin Islands have led a campaign to work together with the private sector to foster development of legitimate businesses within the nation. Livia Freeman, IBA Anti-Money Laundering Forum/British Virgin Islands (Nov. 1, 2010), http://www.anti-moneylaundering.org/northamerica/British_Virgin_Islands.aspx.

Many of these countries have very recently enacted stricter legislation concerning the formation of shell companies. For instance, the Isle of Man has given greater power to its law enforcement to conduct financial reviews when individuals are suspected of criminal activity. Gary Youinou, Know Your Country (Oct. 26, 2011), http://www.knowyourcountry.com/isleofman1111.html. Also, in 2007 Bermuda created the Financial Intelligence Agency (FIA) as an independent agency to investigate suspicious financial activity on the island nation. For a more complete history of the FIA and its powers, see http://www.fia.bm/.


Incorporation Transparency and Law Enforcement Assistance Act, S. Res. 1483, 112th Cong. (2011). Senator Levin has introduced the Act in several previous congresses, but each time the bill has failed to even be passed out of committee. See http://www.govtrack.us/congress/bills/112/s1483.

See Figure 4 and Appendix C, Table 3. In the domestic sample, nearly six percent of firms were still found Non-Compliant when a request was sent from a source with obvious indicators of terrorism.
disconcerting. U.S. states like Delaware compete with tax haven nations to attract business clients. But they have chosen opposite approaches, with Delaware leading a race to the bottom of noncompliance and the tax havens maintaining the most strict compliance with international regulations that aim to stop terrorism and corruption. Indeed, these findings demonstrate that with a higher level of commitment by a government and close collaboration with the business sector, greater compliance results, even in states or nations that work competitively to attract business clients.

A greater commitment by government will come with more stringent identity reporting requirements. And an essential component of government oversight is informing financial institutions of KYC requirements and the criteria for “suspicious” transactions. 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 focusing on complying with regulations. But such efforts will be ineffective if the United States does not also work with other nations to mutually enforce identity requirements in forming shell companies, avoiding an international race to the bottom. 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. Indeed, domestic regulation is far more effective than international regulation at enforcing identity requirements.

---

220 Lacey & George, supra note 116, at 347.
221 Id. (“Financial institutions have as much interest in preventing terrorist attacks as any other sector of society and their potential contribution as experts in financing should be harnessed as effectively as possible. 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.”)
222 Furthermore, regarding anti-money laundering standards to fight terrorist financing, the need for international cooperation and uniformity is incredibly important. Id. at 349.
223 In order to make international regulations more effective, we must “re-conceptual[ize] the public good of open financial systems as having negative security externalities that must be collectively managed.” Clunan, supra note 57, at 570. Collective management will no doubt be difficult, but one common suggestion is to create “a multilateral organization…to draft a comprehensive anti-money laundering convention, and then have signatory nations to the convention adopt implementing domestic legislation.” Id. at 349–50. Such a convention “could incorporate basic anti-money laundering tenets such as criminalizing the act of money laundering and establishing financial institution reporting requirements. Additionally, the convention could…expand the definition of financial institutions to include casinos and entities that allow credit card gambling, 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
mutual implementation of identity reporting requirements will undoubtedly prove difficult, domestic regulation is crucial if nations wish to prevent the funding of terror.

implementing legislation are a necessary component to the effectiveness of a multilateral treaty.”) This would, in turn, help increase compliance on the domestic front.
APPENDIX

APPENDIX A: EXAMPLE E-MAILS

Placebo/Control E-mail

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. I have contacted you because I have several international clients in your region. Recently, our business has grown and tax 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.

Lennart Andersson

Treatments

1. Corruption

Dear Business Incorporation LLC:

I am writing to ask about the possibility of creating an international company. I live in Uzbekistan and I do consulting work with some colleagues here. We focus specifically on public-sector consulting for government procurement. We have started doing quite a bit of foreign work, including in your area, and we have reached a point where it makes sense for us to open up a corporation, both to decrease tax obligations and limit liability. We would like to form a new company in your area as private individuals.

We want to ask you what you need from us to set up such a corporation.
What are your rates? Also, we want to know what identifying documents will be required. Privacy is very important to us, and we would like to set this up in a way that will keep this as confidential as possible, in case of any complications down the road.

We travel a lot, so it makes most sense to continue our communication through email. Your timely response would very much be appreciated.

Sincerely,

Abdullo Ogorodov

2. Terrorism

Dear Incorporation Value Company:

My name is Ahmed Haddad. I am a 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. 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.

Ahmed Haddad

APPENDIX B: RESPONSE E-MAILS

Indignant Response

Dear Mikkel

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

I will be leaving you nothing in my will.

Response to Premium Treatment

Your started 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?”

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 licence 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 the persons giving the same. Please remit half of the fee at this time (see wire instructions below).

Non-Compliant Response

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.

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

**APPENDIX C: RESPONSE DATA**

Tables 2 and 3 below present the international and domestic compliance results. We also cataloged responses as Non-Compliant, Part-Compliant, Compliant, Refusal, and No Response. The table then compares the compliance results across each of the treatments. Proportions that are statistically significant when measured against the benchmark placebo are indicated in bold at the .05 level and italics at the .1 level. The .05 level means, in essence, that there is 1/20 probability that the results were produced by random chance that by a meaningful treatment effect. The .1 level shows an increased probability at 1/10.

**Table 2:** Experimental results by treatment and outcome category for the international samples. In each cell, we include both the total no. of observations and its associated percentage of CSPs. Bolded entries are significant at the .05 level; those in italics at .1.

<table>
<thead>
<tr>
<th>Treatment</th>
<th>Total</th>
<th>Non-Compliant</th>
<th>Part-Compliant</th>
<th>Compliant</th>
<th>Refusal</th>
<th>No Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Placebo</td>
<td>1118</td>
<td>97 (8.68%)</td>
<td>184 (16.46%)</td>
<td>211 (18.87%)</td>
<td>124 (11.10%)</td>
<td>502 (44.90%)</td>
</tr>
<tr>
<td>FATF</td>
<td>391</td>
<td>35 (8.95%)</td>
<td>64 (16.37%)</td>
<td>66 (16.88%)</td>
<td>36 (9.20%)</td>
<td>190 (48.59%)</td>
</tr>
<tr>
<td>Premium</td>
<td>381</td>
<td>23 (6.04%)</td>
<td>67 (17.59%)</td>
<td>54 (14.17%)</td>
<td>47 (12.34%)</td>
<td>190 (49.87%)</td>
</tr>
<tr>
<td>Penalties</td>
<td>383</td>
<td>29 (7.57%)</td>
<td>74 (19.32%)</td>
<td>61 (15.93%)</td>
<td>29 (7.57%)</td>
<td>190 (49.61%)</td>
</tr>
<tr>
<td>Corruption</td>
<td>429</td>
<td>38 (8.86%)</td>
<td>60 (13.99%)</td>
<td>65 (15.15%)</td>
<td>36 (8.39%)</td>
<td>230 (53.61%)</td>
</tr>
<tr>
<td>Terrorism</td>
<td>425</td>
<td>23 (5.41%)</td>
<td>47 (11.06%)</td>
<td>65 (15.29%)</td>
<td>43 (10.12%)</td>
<td>247 (58.12%)</td>
</tr>
</tbody>
</table>

**Table 3:** Experimental results by treatment and outcome category for the domestic samples. In each cell, we include both the total no. of observations and its associated percentage of CSPs. Bolded entries are significant at the .05 level; those in italics at .1.

<table>
<thead>
<tr>
<th>Treatment</th>
<th>Total</th>
<th>Non-Compliant</th>
<th>Part-Compliant</th>
<th>Compliant</th>
<th>Refusal</th>
<th>No Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Placebo</td>
<td>829</td>
<td>92 (11.10%)</td>
<td>13 (1.57%)</td>
<td>3 (0.36%)</td>
<td>106 (12.79%)</td>
<td>602 (72.62%)</td>
</tr>
<tr>
<td>FATF</td>
<td>549</td>
<td>54</td>
<td>11</td>
<td>2</td>
<td>62</td>
<td>417</td>
</tr>
<tr>
<td>Category</td>
<td>Code</td>
<td>Amount</td>
<td>IRS %</td>
<td>Corruption %</td>
<td>Terrorism %</td>
<td></td>
</tr>
<tr>
<td>-------------</td>
<td>------</td>
<td>--------</td>
<td>--------</td>
<td>--------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>IRS</td>
<td>553</td>
<td>42</td>
<td>0.36%</td>
<td>1.50%</td>
<td>32</td>
<td></td>
</tr>
<tr>
<td>Corruption</td>
<td>533</td>
<td>54</td>
<td>0.19%</td>
<td>0.19%</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>Terrorism</td>
<td>557</td>
<td>32</td>
<td>0.36%</td>
<td>0.19%</td>
<td>8</td>
<td></td>
</tr>
</tbody>
</table>