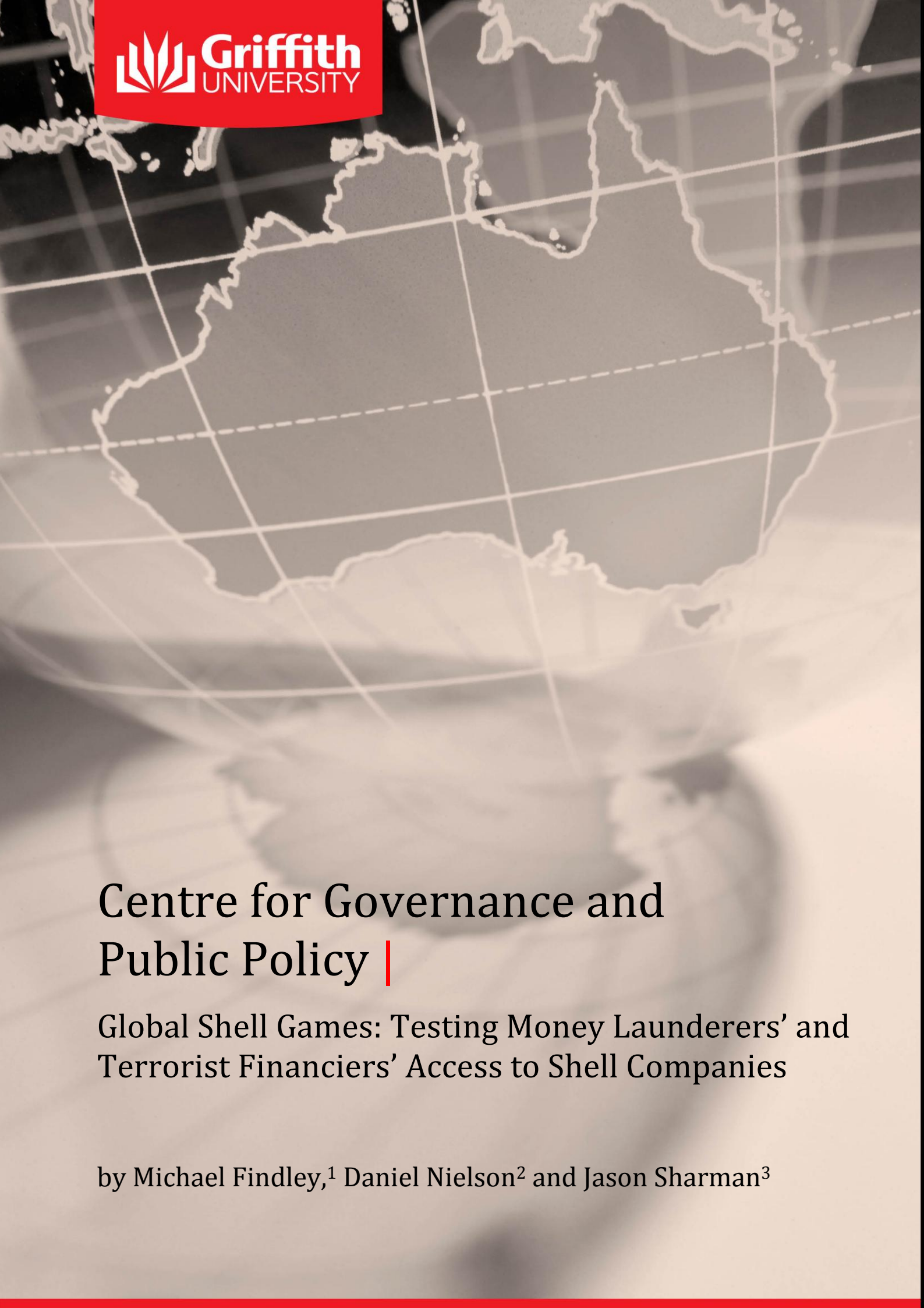


Griffith UNIVERSITY

Centre for Governance and Public Policy |

Global Shell Games: Testing Money Launderers' and Terrorist Financiers' Access to Shell Companies

by Michael Findley,[1] Daniel Nielson[2] and Jason Sharman[3]

Global Shell Games: Testing Money Launderers' and Terrorist Financiers' Access to Shell Companies

by Michael Findley,[1] Daniel Nielson[2] and Jason Sharman[3]

Summary

For criminals moving large sums of dirty money internationally, there is no better device than an untraceable shell company. This paper reports the results of an experiment soliciting offers for these prohibited anonymous shell corporations. Our research team impersonated a variety of low- and high-risk customers, including would-be money launderers, corrupt officials, and terrorist financiers when requesting the anonymous companies. Evidence is drawn from more than 7,400 email solicitations to more than 3,700 Corporate Service Providers that make and sell shell companies in 182 countries. The experiment allows us to test whether international rules are actually effective when they mandate that those selling shell companies must collect identity documents from their customers. Shell companies that cannot be traced back to their real owners are one of the most common means for laundering money, giving and receiving bribes, busting sanctions, evading taxes, and financing terrorism.

The results provide the most complete and robust test of the effectiveness of international rules banning untraceable, anonymous shell companies. Furthermore, because the exercise took the form of a randomized experiment, it also provides unique insight into what causes those who sell shell companies to either comply with or violate international rules requiring them to collect identity documents from customers. Just as the random assignment to control (placebo) and treatment groups in drug trials isolates the effect of a new drug, so too the random assignment of low-risk "placebo" emails and different high-risk "treatment" emails isolated the effects of different kinds of risk on the likelihood of (a) being offered a shell company, and (b) being required to provide proof of identity. Key findings include:[1]

1. Overall, international rules that those forming shell companies must collect proof of customers' identity are ineffective. Nearly half (48 percent) of all replies received did not ask for proper identification, and 22 percent did not ask for any identity documents at all to form a shell company.

2. Against the conventional policy wisdom, those selling shell companies from tax havens were significantly more likely to comply with the rules than providers in OECD countries like the United States and Britain. Another surprise was that providers in poorer, developing countries were also more compliant with global standards than those in rich, developed nations.

3. Defying the international guidelines of a "risk-based approach," shell company providers were often remarkably insensitive to even obvious criminal risks. Thus, although providers were less likely to reply to clear corruption risks, those that did respond were also less likely than in the placebo condition to demand certified identity documents of potential customers from high-corruption countries who claim to work in government procurement.

4. Corporate service providers were significantly less likely to reply to potential terrorists and were also significantly less likely to offer anonymous shell companies to customers who are possibly linked to terror. However, compared to the placebo a significantly decreased share of firms replying to the terrorist profile also failed to ask for identity documentation or refused service.

5. Informing providers of the rules they should be following made them no more likely to do so, even when penalties for non-compliance were mentioned. In contrast, when customers offered to pay providers a premium to flout international rules, the rate of demand for certified identity documentation fell precipitously compared to the placebo.

Global Shell Games

Table of Contents

Introduction

For those engaged in money laundering, sanctions-busting, tax evasion, major corruption, the financing of terrorism and a wide variety of other financial crimes, untraceable shell companies provide a key resource. Such shell companies can be set up online in dozens of countries in days or even hours for as little as a few hundred dollars. Shell companies that cannot be linked back to the real individuals in control create near-insuperable obstacles for regulators and law enforcement officials.

Reflecting the serious dangers posed by the illicit use of shell companies, prominent international organizations have instituted rules specifying that authorities must be able to access information on those who own and control such companies. The extent to which these rules are actually effective, however, is essentially unknown. We do not know how difficult or easy it is to obtain an untraceable shell company or what makes those who sell shell companies more or less likely to follow the rules requiring proof of customer identity. This study provides the best available answers to these questions and thus aims to improve policy devoted to countering the illicit uses of shell companies.

The basis of the study was to impersonate 21 fictitious consultants representing various risk profiles, and then make more than 7,400 email solicitations for shell companies to more than 3,700 Corporate Service Providers in 182 countries. The outcomes of interest were, first, whether these providers responded with an offer of a shell company and, second, what identity documents they required, if any. If the international rules were effective, providers would have required notarized identity documents from customers and applied enhanced scrutiny to customers with a high-risk profile.

Given the centrality of untraceable shell companies for the crimes listed above, our findings about how easily these prohibited companies are available, even to obviously high-risk clients, are of serious concern. Overall, 48 percent of the replies received failed to comply with international rules on customer identification, and 22 percent failed to require any proof of identity at all.

Running directly counter to conventional policy wisdom on the subject, providers based in tax haven countries were significantly *more* likely to follow the rules, to apply the "Know Your Customer" principle, than those in non-tax haven countries. Another surprise was that providers in poorer, developing countries were at least as compliant as those in rich, developed countries.

Directly contradicting the principle of the "risk-based approach," which supposedly governs company formation, providers were remarkably insensitive to even very obvious corruption risks. Although such risky customers were less likely to get a reply, providers were also significantly less likely to demand certified identification. Services were more vigilant with potential terrorists, but even there they asked for identity documents at significantly lower rates, and sometimes explicitly offered anonymous incorporation. For example, one provider responded to a terrorist financing risk customer by saying "It sounds like you want to form your company anonymously with the State, is that correct? We can do that for an extra $25. If we are

just setting up a Corporation for you and that's it we don't require any documents from you at all."

Telling providers about the rules they should be applying made them no more likely to do so, even in cases where approach emails mentioned penalties for non-compliance. On the other hand, offering to pay providers a premium *not* to apply the rules did in fact encourage significantly fewer providers to follow these rules.

We summarize all these results in a "Dodgy Shopping Count," which shows on average how many providers a particular kind of customer would have to approach before being offered an untraceable shell company.

These results present a far more accurate and robust picture of the true state of affairs on shell companies and the effectiveness of the international rules that supposedly govern them than any previous study. The cases of shell-company enabled crimes that come to the attention of law enforcement or the media are by definition unrepresentative, simply because they have become public. International organizations and government agencies often try to assess policy effectiveness by either just reading the rules on the books, which may have limited correspondence to what actually happens in practice, or by counting successful prosecutions or totals of dirty money seized, which again gives little idea as to how many violations occur without official notice.

Isolated attempts to engage in similar sorts of solicitation exercises by journalists and academics provide a somewhat better indication of the ease with which would-be criminals can come by untraceable shell companies,[2] but still suffer from severe limitations compared with this study. These earlier solicitations have either been for one or a few shell companies, or at most in the dozens. In contrast, our conclusions rest on 7,466 approaches to 3,773 providers in 182 countries. Perhaps even more importantly, this study uses deliberately differentiated approaches to test what makes providers more and less likely to comply.

The remainder of this paper is divided into seven sections. The first explains what shell companies are, why they are important in financial crime, and what kinds of businesses sell them. The second describes the international rules that (in theory at least) govern shell companies to ensure that authorities can "look through" the corporate veil to find those individuals in control. The next section explains how we designed the study, how we compiled our list of providers but especially the design of the various email approaches and fictitious personas. The fourth part explains the interpretation and classification of the email correspondence received. The fifth section briefly explains why the random assignment of different customer-risk profiles allows us to tell what causes higher and lower rates of compliance. The sixth section presents the results of the study, with the material broken down to separately address four issues. These relate to global patterns of compliance and non-compliance; relative compliance among tax havens, developed and developing countries; the effects of different risk profiles on response and compliance rates; and the effects of information, penalties and inducements on providers' willingness to follow or break the rules. Finally, we briefly discuss the legality and ethics of our study.

What are Shell Companies, Why do they Matter, and Who Sells Them?

At most basic, in the eyes of the law all companies are simply a "legal person," which, like real people, can sue and be sued, hold bank accounts, and own and sell property and other assets. In contrast to operating or trading companies that have employees who make a product or provide a service, however, shell companies are little more than this legal identity, and hence the "shell" moniker. Any country or jurisdiction that allows for the formation of companies almost by definition allows for the creation of shell companies, which take on the nationality of this jurisdiction. Although it varies from place to place, shell companies are often quick and easy to set up, obtainable within a few hours or days and costing between a few hundred and a few thousand dollars. A large majority of shell companies are used for completely legal and legitimate purposes – for instance, as a holding company. However, a significant minority are central to a wide range of criminal enterprises.

Shell companies are a threat when they cannot be traced back to the real person or people in control. Anonymous shell companies are so useful to criminals because they screen or veil illicit conduct. Because the companies themselves are largely expendable, it does little good if law enforcement officials can follow some criminal enterprise or trail of illicit funds back to a company, but no further. The defining metaphor is of shell companies functioning as a "corporate veil": screening and separating criminals from illicit financial activities.[3] Thus the crux of the issue is whether authorities can "look through" the corporate veil to find the individuals pulling the strings (referred to as the "beneficial owner"). There are many instances of shell companies' being used in criminal schemes, with some examples presented below.

- In December 2009 a plane searched in Bangkok was found to be carrying North Korean arms bound for Iran, in violation of international sanctions. The plane had been leased by a New Zealand shell company, but there was no information on the individual who controlled the company.[4]

- The Iranian government used shell companies from Germany, Malta, and Cyprus to evade international sanctions by concealing the ownership of its oil tankers.[5]

- The British arms firm BAE Systems pleaded guilty in 2010 in connection with case which saw it pass secret funds through a series of middle-men and shell companies incorporated in Britain and the British Virgin Islands to key Saudi officials responsible for approving a massive arms purchase from BAE.[6]

- Teodorin Obiang, son and heir-apparent of the president of the oil-rich West African nation of Equatorial Guinea, laundered corruption proceeds in the United States by using a series of Californian shell companies to hold bank accounts and title to his $35 million Malibu mansion.[7]

- Corrupt Russian tax officials used shell companies from Cyprus and the British Virgin Islands to steal hundreds of millions of dollars in a case that led to the imprisonment and death of Russian whistle-blower Sergei Magnitsky.[8]

- Recent cases against Swiss banks like UBS and Wegelin have often turned on the tendency of American clients to evade US tax obligations by the ruse of holding their accounts through shell companies controlled by these clients.[9]

- Russian arms dealer Viktor Bout was convicted in November 2011 of conspiracy to provide aid to a terrorist organization. Bout's illicit activities were crucially dependent on a network of shell companies in Texas, Delaware, Florida, and elsewhere around the globe.[10]

- The Mexican Sinaloa Drug Cartel employed New Zealand and other shell companies to launder tens of millions of dollars of cocaine profits through Latvian banks.[11]

As a result of these and many other instances, time and time again international organizations, national governments, and NGOs have emphasized that progress in combating these and other financial crimes depends on the effective regulation of shell companies, especially in terms of being able to establish the link back to the beneficial owners.[12]

In most of these cases Corporate Service Providers (CSPs) acted as crucial intermediaries supplying individual clients with shell companies.[13] These firms make a living by receiving orders for shell companies from clients, lodging the official paperwork, and paying the government fee necessary to create a company. They also offer various auxiliary services, ranging from virtual office facilities to filling important corporate roles as nominee directors, secretaries, or shareholders. CSPs may be sole traders forming companies on a bespoke basis, or wholesalers responsible for the formation and on-going support of tens of thousands of companies through a network of dozens of associated retailers.[14] These firms may be law or accounting firms creating shell companies on an incidental basis, or specialized concerns that do little else. As described below, CSPs are the crucial point at which regulators may intervene to impose a duty to collect customer identity documents.

What are the Rules Governing Shell Companies and How are they Meant to Work?

The international standard governing shell companies is clear-cut. It states: "Countries should take measures to prevent the misuse of legal persons [i.e., companies] for money laundering or terrorist financing. Countries should ensure that there is adequate, accurate and timely information on the beneficial ownership and control of legal persons that can be obtained or accessed in a timely fashion by competent authorities."[15] This rule has been set down by the Financial Action Task Force (FATF), the world's standard-setter and enforcer of anti-money laundering standards. The FATF was founded in 1990 and has been dominated by developed states, more recently augmented by powerful transitional and developing countries like Russia,

China, India and Brazil. Over 180 countries have committed to FATF standards, which have also been endorsed by the UN, G20, World Bank and many other bodies.[16]

In principle, there are three ways to establish the beneficial owner of shell companies: through strong law enforcement powers, company registries, or Corporate Service Providers,[17] though we argue that only the last provides a realistic solution.

The first potential option is for law enforcement agencies to have strong investigative powers to track down shell company owners. The difficulty here, however, is that police powers are limited by national jurisdictions, whereas the misuse of shell companies is all too often an international problem. The shell company may be incorporated in a different jurisdiction, or the beneficial owner may be a foreign resident, or the provider may be located in a different jurisdiction, or all three. Furthermore, if the provider who formed the company did not collect any information on the owner (as our results show is common), no amount of police pressure will summon up the missing information. As one provider replied to one of our earlier solicitations: "Regarding confidentiality, no information is taken, so none can be given. It is that simple!"

The second option might seem the most promising: having government company registries collect and file information on the real owners. If companies are creatures of law, they cannot exist without some documentation lodged with some form of company registry. From here it might seem an easy step to simply require these registries to demand and hold owners' proof of identity. Company registries, however, largely have a passive, archival function of collecting a very limited range of information. Though some registries hold more information on companies than others, currently to our knowledge only one, that in Jersey, holds the information on the beneficial owner.[18] Few if any registries have the capacity or desire to change this state of affairs.

By elimination, this leaves the third option, requiring CSPs to collect and hold identity documentation on customers forming shell companies according to the "Know Your Customer" principle. In practice, this is the only way to reliably establish the real owner of shell companies. This solution depends on licensing and regulating providers (something which many countries, including the United States, do not do), imposing a legal duty on them to collect proof of identification from customers, and auditing providers to make sure they do in fact collect this information, with penalties for non-compliance. Because law enforcement powers are largely limited by national boundaries, and because company registries do not collect beneficial ownership information, in practice, if CSPs do not establish the real owner of shell companies, no one else will. This is why CSPs are at the heart of our study.

The major advantage of ensuring the ability to "look through" shell companies by regulating those that sell them is that it actually works. As discussed in the results section below, several countries that regulate CSPs had near-perfect records of asking for identity documents from our fictitious customers.

The Design of the Study: Finding Providers and Composing Treatments

Two of the most important aspects of the design of the study were compiling the list of shell company providers to approach and designing the different email solicitations. Here we explain each step in turn.

As noted above, CSPs are not regulated in many jurisdictions, so any person or firm can form and sell shell companies. This means that there is no definitive list of those selling shell companies. Thus the list of providers we approached was compiled by Google searches for "company formation," "business law" and cognate terms for every country in the world. These searches resulted in a pool of 3,773 providers in general, of which 1,785 were from the United States, 444 from other OECD countries, 505 from tax havens, and 1,039 from non-tax haven developing countries. Two experiments were conducted: one on an international sample where a small number of U.S. providers were included and another on an exclusively U.S. sample. Of the 1,785 U.S. providers, 63 were in the international sample and 1,722 were in the U.S. sample. Because the two experiments were conducted separately, we generally report the results of each on their own.[19] Though this does not represent every provider, it does capture a large share of those engaged in international company formation.

The next step was to design the different email messages to be sent to CSPs. These were built around a common frame, but also included key differences. First, all of the fictitious customers were consultants, on the grounds that this is a plausible reason a person would legitimately seek a shell company, but also because it is a common cover story for those looking for an alibi for the proceeds of crime.[20] The next common element was the specific rationale for wanting a shell company, revolving around limiting legal liability, reducing "excessive" taxes, and preserving confidentiality. From interviews conducted in countries including the U.S., the UK, Switzerland, Singapore, Hong Kong, the British Virgin Islands, Panama and the Cayman Islands, as well as from attending CSPs' industry conferences, these are the most common reasons people form shell companies. Finally, each approach asked how much a company would cost and, crucially, what identity documents were necessary to have a company formed. Beyond this common frame, we introduced important differences to test the response to different kinds of customers, different amounts of information, and different levels of risk.

The first approach was the placebo or "control" email. In this version the consultant hailed from one of eight relatively small, rich countries with low levels of perceived terrorism and corruption risk, and which are not regarded as tax havens: Australia, Austria, Denmark, Finland, the Netherlands, New Zealand, Norway and Sweden, for convenience labeled the "Norstralia" countries. We used eight countries for the placebo rather than just one to guard against the possibility that some serious scandal or chance event might change the general perception of one of the countries during the study, and thus skew the results. Each country was associated with a single alias, drawn from the most frequent male names in the relevant culture. For the aliases hailing from countries where English is not the native language, we introduced two spelling, grammar, or syntax errors to enhance authenticity. One example reads:

“Dear Rapid Filing Inc.:[21]

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”

The control email served as a crucial benchmark for the rest of the study. We measured the rate at which providers replied to the approach, and the rate at which they asked for identity documentation, and then used these measures as a baseline or yardstick to compare how changing the information in the email caused changes in the response rate (whether or not providers replied) and the likelihood of being asked for proof of identity (the compliance rate).

In total we used 12 different kinds of email approaches, or experimental conditions. These are summarized in Table 1 below, though we only discuss the first 7 here.

Table 1: Experimental Conditions

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

The first variation was intended to learn if raising the corruption risk made a difference to providers' willingness to sell shell companies and ask for proof of identity. We did this by altering first the nationality of the consultant, and then the industry. Instead of the low-corruption "Norstralia" countries, we used eight relatively indistinguishable countries widely perceived to have high levels of corruption: Guinea, Guinea-Bissau, Equatorial Guinea, Papua New Guinea, Kyrgyzstan, Tajikistan, Turkmenistan and Uzbekistan, abbreviated as the "Guineastan" countries.[22] International standards caution providers to apply particular scrutiny to customers from corruption-prone countries.[23] To raise the corruption risk even further, the consultants claimed to work in government procurement, one of the most corruption-prone areas.[24] In combination, a customer from a high-corruption risk country, working in a high-corruption risk industry, wanting to buy a shell company to enhance financial secrecy should have been an obvious signal of corrupt intent to providers. Thus one example reads:

“Dear Business Incorporation LLC:

I am writing to aks 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 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”

The second treatment was intended to raise a terrorism financing risk. Here the consultants were citizens from one of four countries perceived to have a high risk of terrorist financing: Lebanon, Pakistan, Palestine and Yemen.[25] Furthermore, these individuals claimed to work in Saudi Arabia for a Muslim charity, another conspicuous terrorist financing risk factor according to international guidelines.[26] Again, the combination of individuals from a country perceived to play host to terrorist groups, working for a Muslim charity, and seeking financial secrecy poses a very unsubtle terrorist financing risk.

“Dear Incorporation Value Company:

My name is Ahmed Haddad. I am 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"

The third treatment added to the basic template by informing providers of the international identification standard they should be following to see whether this made any difference to their inclination to comply, while the fourth and fifth treatments included this same information, but also mentioned the prospects of sanctions enforced by the Financial Action Task Force or, for U.S. providers, the Internal Revenue Service. Our expectation was that these treatments would raise the proportion of CSPs complying with international rules by requiring identity documents, and/or perhaps lowering the number willing to do business.

The final treatment discussed here involved adding a sentence to offer providers an extra payment if they waived the requirement to ask for identity documents. On common-sense grounds, those offering to pay others to violate rules should raise suspicions, but in addition international guidelines specifically warn against clients who are prepared to pay such a premium.[27] The question was whether the effect would be to lower response rates and increase compliance rates, as CSPs picked up on the risk involved in such a dubious offer, or vice versa, if CSPs were tempted by the extra payment.

All email approaches were made from dedicated Internet email accounts registered to mobile phone numbers purchased in an African country. All emails were sent out by researchers based in the United States, but this point of origin was disguised by the use of proxy servers to make it appear the emails came from various countries in Europe and East Asia. Where no reply was received within roughly one week, a follow-up email was sent. When replies did not answer the question of what identity documents (if any) were required, a specific prompt was sent to elicit this information.

Coding Responses: What Counts as Compliant and Non-Compliant?

The next major task was to decide which email responses to our solicitations counted as compliant or non-compliant with the rule that shell companies must be able to be traced back to their real owners. There were five possible outcomes, explained below: no response, non-compliant, partially compliant, compliant, and refusal.

No response is largely self-explanatory, but as we discuss in the Results section, we later worked to find out to what extent those who did not reply were engaged in a form of risk avoidance by simply not engaging with suspicious customers.

CSPs may have refused for a variety of reasons, from commercial grounds, to excessive workload, to a judgment that these potential customers involved too much risk. Some refusals were indignant and thought our approach was a scam:

“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, fraudelent [sic] buck at the expense of others, then please spare a thought for the prospect you will remain a complete, impoverished idiot for the reseof [sic] your life and die poor and sad.

I will be leaving you nothing in my will.”

Others were tongue-in-cheek, and a few threatened to report the approach to the police. Sometimes in refusing the riskiest customers providers indicated that a “no” might be changed into a “yes” if the price were right, as the following reply from a U.S. provider to our terrorism financing risk suggests:

“[Y]our 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?”

To be counted as compliant, a CSP reply had to ask for some form of notarized or certified copy of a government-issued photo identity document. Usually, this would be a notarized scan of a picture page of the customer’s passport, often supported by utility bills to show proof of residence. CSPs would then hold this copy on file, so that if local or foreign law enforcement authorities later wanted to find out who was behind the company they could require the CSP turn over this information. In this way, the authorities have the ability to pierce the corporate veil should the need arise. This is a typical example of a compliant response from a provider in St Kitts:

“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).”

Partially compliant responses required some identification, but did not meet the standard of notarized copies of government-issued photo identity documents. While this might give the authorities something to go on in tracking down the real owner of the shell company, it provides less information and is easier to fake.

Non-compliant responses offered to provide a shell company with no need to supply any identity documents at all. As a result, the resulting company would be exactly the sort of untraceable entity that is so useful for money launderers, corrupt officials, and the financiers of terrorism, as discussed earlier. The trail stops after the CSP and the shell company. A few examples of non-compliant responses from U.S. providers are presented below:

"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!"

To ensure reliability, all email responses were coded twice by two separate coders in accordance with a formal manual. When discrepancies arose, a senior researcher arbitrated the codes and assigned a final value.

Why Randomly Assign Emails? The Logic of Experiments

Central to our project is the random allocation of different emails among the pool of providers. The reason behind this approach is to find out what causes CSPs to be more or less compliant with the rules on shell companies by mimicking the logic of randomized drug trials. In order to find out whether a particular new drug is effective in fighting some disease, and if the drug causes harmful side effects, it must be subject to a randomized clinical trial.

A pool of volunteers are randomly assigned to receive either the drug in question (the treatment group) or a placebo pill (the control group). Subsequently, any positive or negative average differences in the health of the two groups can be wholly and solely attributed to the effects of the drug in question. The random allocation of the subjects to either the control (placebo) or treatment groups "washes out" or neutralizes all the other average differences between groups (other health conditions, genetic differences, life-style differences, etc.). As random assignment means that individuals with particular types of risk factors should be evenly distributed to control and treatment groups, the effects of these other factors should balance out when comparing the two groups after the trial. Any difference between the two groups afterwards has been caused by the drug. This method of random allocation to control and treatment groups is the basis of all scientific experiments, and it is the best way of finding out what causes what.

How does this logic apply to our shell company project? Here, rather than a placebo pill we have the placebo email from the Norstralian consultants described above. Rather than a drug as the

treatment, we have the variety of treatment emails listed in Table 1. Like the pool of medical volunteers, we randomly allocate providers to one or other of the different emails. Because we have a very large pool of CSPs, we can be confident that all the other factors that affect providers' willingness to respond to the emails and their likelihood of enforcing the "Know Your Customer" requirement are balanced across the conditions.[28] Differences in the response and compliance rates between the placebo and the various treatments reflect only the varying information in the email concerning customer risk, possible penalties, and so on. The response and compliance rates to the placebo email thus act as a baseline; if there are differences in these rates for the other email treatments compared with the placebo email, the difference are attributed to the changes we introduced in the email and not other, outside factors.

Results and Findings

We group the main results into four clusters: first, the overall, global effectiveness of the "Know Your Customer" rule requiring that providers collect proof of identity; second, relative compliance rates of tax havens, rich and developed OECD countries, and poorer developing countries; third, the (in)sensitivity of providers to corruption and terrorism financing risks; and, finally, the effects of more information about the rules, and penalties and inducements for breaking them. After detailing each of these responses we also explain the significance of non-responses.

We explain many of these results with reference to a "Dodgy Shopping Count," which measures the average number of providers a particular type of customer would have to approach to receive a non-compliant response, i.e., be offered a shell company with no need to supply any identity documents. A 5 percent non-compliance rate would thus equal a Dodgy Shopping Count of 20. The lower the Dodgy Shopping Count, the easier it is to get an anonymous shell corporation.

As discussed above, there is a clear international rule mandating that authorities have "adequate, accurate and timely information" on the real owners of any given shell company. In practice, they can only do so if providers collect identity documents. Whether or not this rule actually works matters greatly in fighting the range of financial crimes listed earlier. Yet until our study, policy makers have in effect had no idea whether or to what extent this rule is actually observed in practice. Clearly, even if there is a law committing incorporation services to identify customers, providers may or may not be following it.

At the broadest level including the placebo email and all of the treatments, of the 7,466 inquiries sent, the non-compliance level for the international sample (with the 63 U.S. firms) is 8.4 percent, for an overall Dodgy Shopping Count of 12. The 8.4 percent includes non-responses in the denominator, since some CSPs may fail to reply in response to risk and thus may be complying with international law in a "soft" way. In the United States sample, the noncompliance level is 9.2 percent and the Dodgy Shopping Count was 10.9, which was almost 10 percent lower than the average in the international sample. Obtaining an anonymous shell company is therefore easier in the U.S. than in the rest of the world.

However, two factors worsen the gap between the U.S. and other countries. First, the U.S. number is elevated by the much higher non-response rate from firms in U.S. sample, which was

77.3 percent in the U.S. compared to 49.3 percent in the international sample. The proportion of providers in the U.S. sample who replied to our inquiries *and* required no identity documents whatsoever was 41.5 percent, which is roughly two-and-a-half times the average of 16.5 percent in the international sample. We followed up with firms failing to reply to any of our emails with an innocuous inquiry basically asking if the firm was still in business and assisting customers but making no mention of confidentiality, taxes, or liability. We learned that the vast majority of non-responses are not soft refusals: they failed to respond to any inquiry, even the most innocuous that we could design.

Second, there is a substantial difference between U.S. business law firms and incorporation services in their compliance rates, as well as major variation in compliance among U.S. states. See Figures 2 and 4 below. Business law firms also replied at much lower rates than other U.S. providers (16.6 percent in the United States sample compared with 55.5 percent of U.S. incorporation services). Furthermore, these other providers were especially unlikely to ask for any identity documents from potential customers. In general, however, only a tiny proportion of U.S. providers of any kind met the international standard by requiring notarized identity documents (10 of 1722 in the U.S. sample, or a proportion of 0.00058). There was considerable variation between different states as to whether providers asked for any customer identification. Wyoming, Delaware and Nevada were among the worst in being the most likely to supply untraceable shell companies, a particularly worrying finding in that providers in these states are most likely to sell companies to foreign clients.

Table 2 below presents the overall global results of the replies received as well as those for the United States broken down by Non-Compliant, Partially Compliant, Compliant, Refusal, and No Response. The table compares rates across the different experimental conditions, with proportions that are different from the Placebo in a statistically significant way indicated by boldface at the .05 level and by italics the .1 level. The .05 level effectively means that there is a 1 in 20 probability that the results were produced by random chance rather than by a meaningful treatment effect. This is the typical standard in social science. The less-stringent .1 level indicates a 1 in 10 chance of the result being produced by random chance rather than suggesting a real effect.

Table 2: All Experimental Results by Treatment and Outcome Category for International and U.S. Samples. In each cell, we first include the total number of observations along with the associated percentage underneath. Entries in bold are different from the Placebo at the 0.05 level of statistical significance. Entries in italics are significant at the 0.1 level.

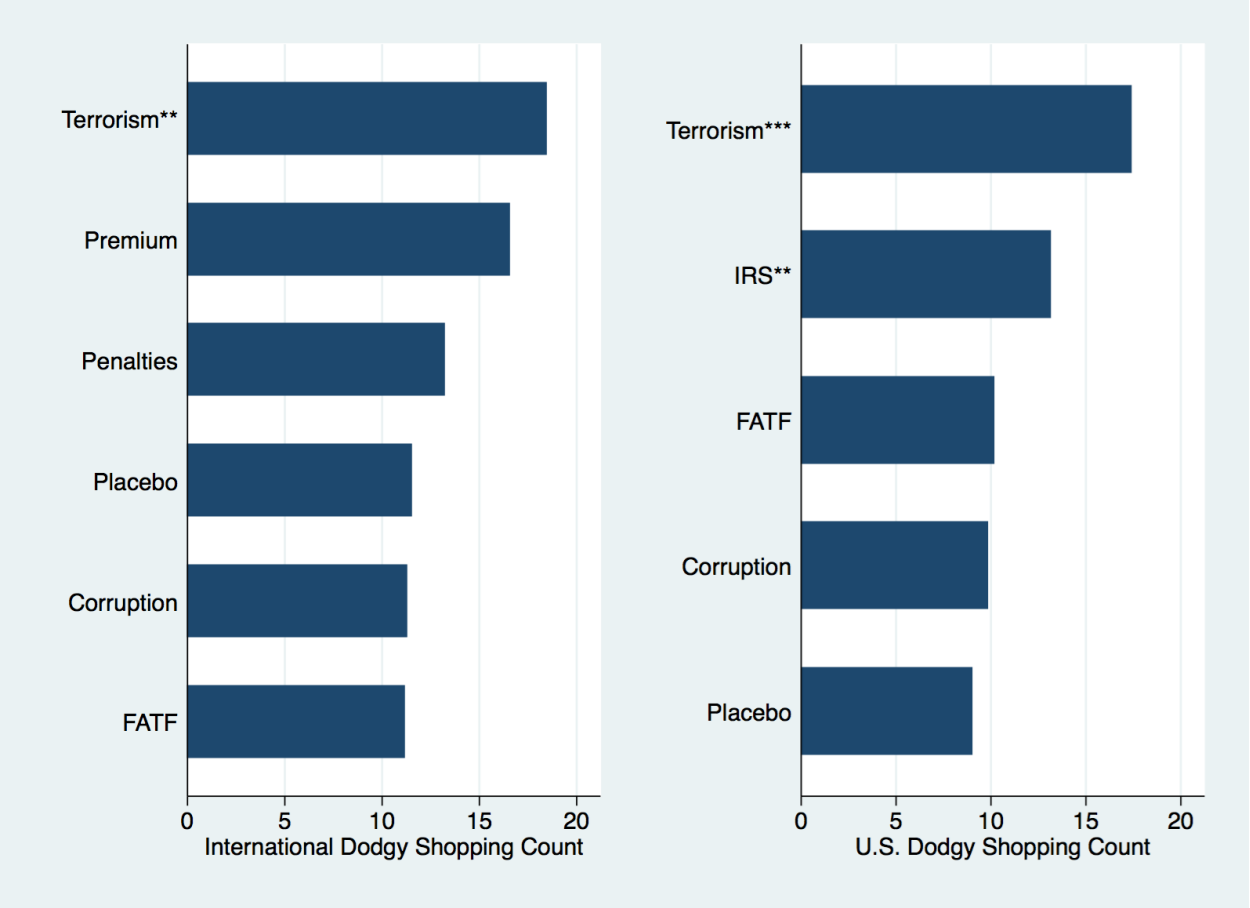
INTERNATIONAL SAMPLE

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

UNITED STATES SAMPLE

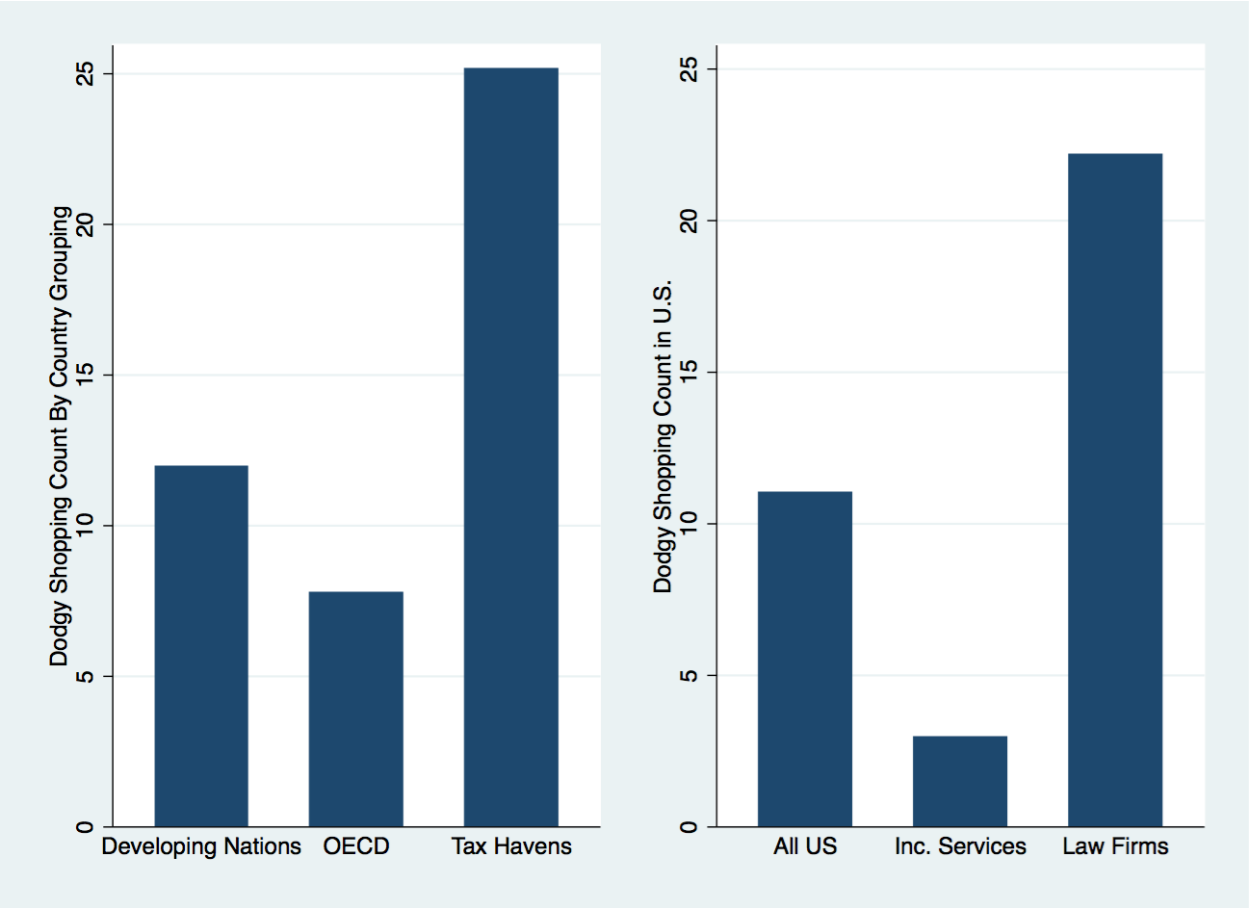
Treatment	Total	Non-Compliant	Part-Compliant	Compliant	Refusal	No Response
Placebo	829	92	13	3	106	602
		11.10%	1.57%	0.36%	12.79%	72.62%
FATF	549	54	11	2	62	417
		9.84%	2.00%	0.36%	11.29%	75.96%
IRS	553	**42**	12	2	*54*	**442**
		7.59%	2.17%	0.36%	*9.76%*	**79.93%**
Corruption	533	54	8	1	*52*	**417**
		10.13%	1.50%	0.19%	*9.76%*	**78.24%**
Terrorism	557	**32**	8	2	**50**	**458**
		5.75%	1.44%	0.36%	**8.98%**	**82.23%**

Figure 1: Dodgy Shopping Count by Treatment. International and U.S. results reported separately. Conditions statistically different from the Placebo denoted with asterisks. ***p<0.01; **p<0.05



A finding that runs directly counter to the conventional wisdom is that rich countries in the Organization of Economic Cooperation and Development (OECD) are worse at enforcing the rules on corporate transparency than are poor countries (see Figure 2). For developing countries the Dodgy Shopping Count is 12, while for developed countries it is 7.8 (and tax havens are much higher at 25.2, as discussed below). The significance of this finding is that it does not seem to be particularly expensive to enforce the rules on shell companies, given that poor nations do better than rich countries. This suggests that the relatively lackluster performance in rich countries reflects a simple unwillingness to enforce the rules, rather than any incapacity.

Figure 2: Dodgy Shopping Count by Type of Country Internationally and by Type of Firm in the United States



One of the biggest surprises of the project was the relative performance of rich, developed states compared with poorer, developing countries and tax havens (see Figure 3). The overwhelming policy consensus, strongly articulated in G20 communiqués and by many NGOs, is that tax havens provide strict secrecy and lax regulation, especially when it comes to shell companies. This consensus is wrong. The Dodgy Shopping Count for tax havens is 25.2, which is in fact much higher than the score for rich, developed countries at 7.8 – meaning it is more than three times harder to obtain an untraceable shell company in tax havens than in developed countries. Some of the top-ranked countries in the world are tax havens such as Jersey, the Cayman Islands and the Bahamas, while some developed countries like the United Kingdom, Australia, Canada and the United States rank near the bottom of the list. It is easier to obtain an untraceable shell company from incorporation services (though not law firms) in the United States than in any other country save Kenya.

Figure 3: Dodgy Shopping Count by Country for Nations with at least 25 approaches. All U.S. firms from the U.S.-only sample are included together with the 63 U.S. firms in the international sample. Firms in none of the top eight countries were ever found noncompliant. Because there is no natural upper bound on the Dodgy Shopping Count, we set it to 100 for these. But they should be interpreted as having a record without any noncompliance.

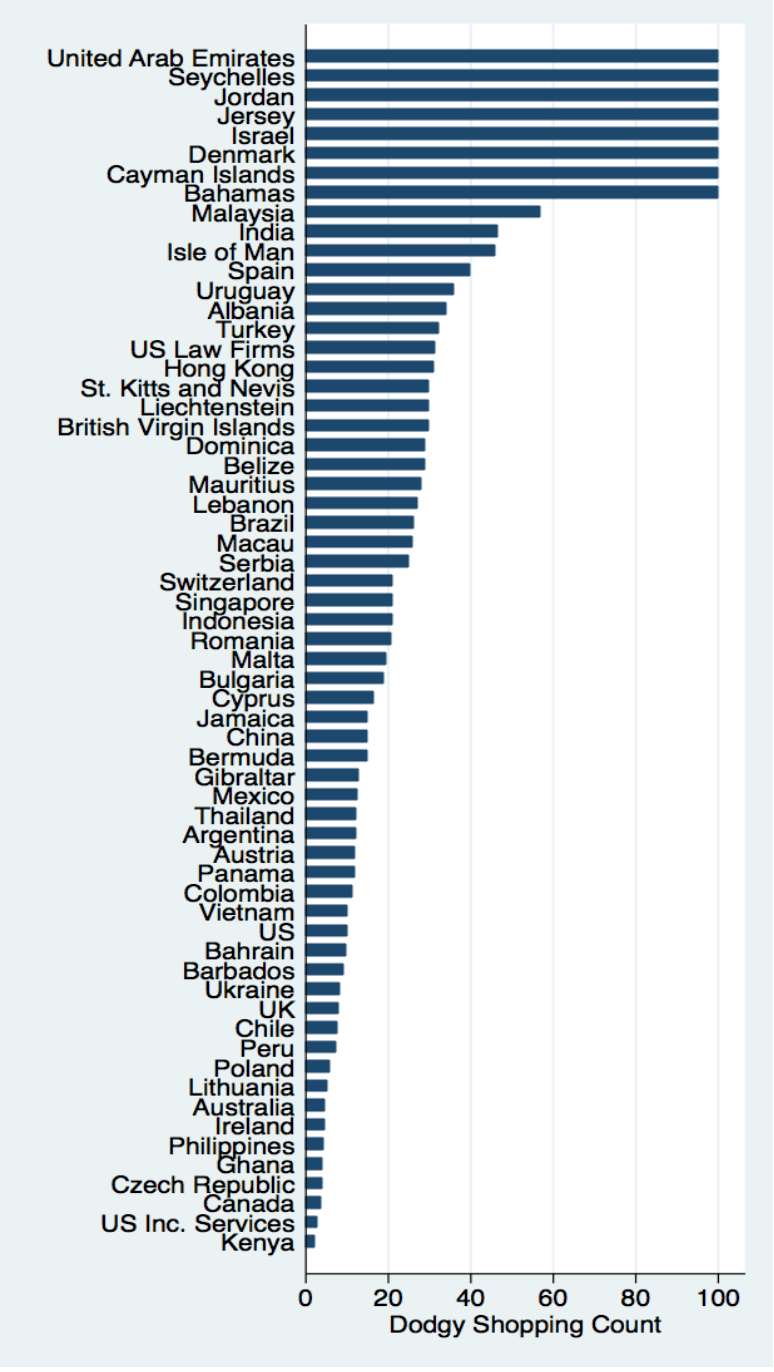
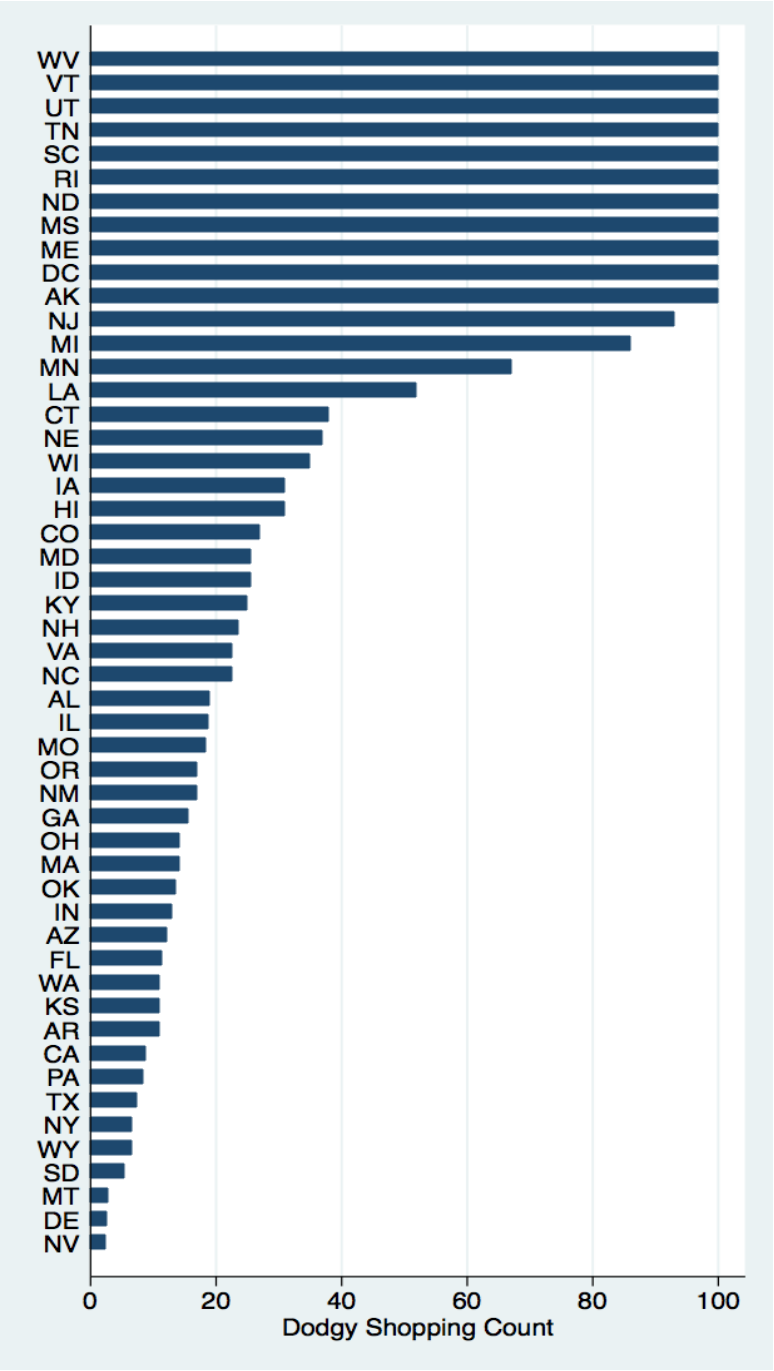


Figure 4: Dodgy Shopping Count by State in the U.S. for all states. Similar to Figure 3, firms in none of the top eleven states were ever found noncompliant. Because there is no natural upper bound on the Dodgy Shopping Count, we set it to 100 for these as well. But they should be interpreted as having a record without any noncompliance.



A final note on the Figures above is that very high Dodgy Shopping Counts (i.e., very low rates of Non-Compliance) in some cases 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 these. Thus, jurisdictions may have highly positive Dodgy Shopping Counts with very different patterns in the other categories.

How much did the different email treatments affect the results? We first consider the Corruption and Terrorism treatments relative to the benchmark Placebo email. In some ways the biggest surprise was how little difference there was between the relatively innocuous Norstralian Placebo email and the obviously high-risk Guineastan treatment signaling corruption, though the Terrorism treatment was substantially different. In the international sample, the Dodgy Shopping Count was 11.5 for the Placebo, 11.3 for Guineastan, and 18.5 for the Terrorism financing risk (the results for the United States are 9 for the Placebo, 9.9 for Guineastan, and 17.4 for Terrorism financing). See Figure 1. Indeed, it is particularly worrying that the obvious corruption risk actually *reduced* compliance significantly (by lowering Compliance rates in the international pool and reducing Refusal rates in the U.S. sample), despite the international guidelines specifying that these customers should be subject to enhanced scrutiny. See Table 2.

The Terrorism financing results are mixed and thus not completely re-assuring. Relative to the Placebo email, the Terrorism finance-risk customers were less likely to receive a reply, suggesting "soft" refusals. Likewise, both the international and U.S. subject pools saw the Terrorism condition cause significantly lower Non-Compliance rates compared to the Placebo, meaning that potential terrorists face a more difficult task in obtaining anonymous shell corporations. However, this is offset by the fact that the Terrorism condition also decreased the Part-Compliance rate in the international pool, meaning that firms were less likely to ask possible terrorists for at least some form of I.D. than in the Placebo condition.

Likewise, potential terrorists received fewer refusals in the United States compared to the Placebo. And since virtually no firms asked for any form of identification in the U.S., refusal was the only way U.S. firms complied with international standards, so a significant drop in the rate of Refusal is worrisome. These findings on corruption and terrorism financing provide evidence that the principle of a "risk-based approach," according to which riskier customers should attract greater scrutiny, is relatively ineffective in screening corrupt customers and only partly effective at thwarting potential terrorists.

The next set of treatments tested three questions. First, does telling providers about the rules they should be following make providers any more likely to follow them? Second, does raising the prospect of penalties make providers any more likely to comply with Know Your Customer rules? This second question was divided into two treatments: in the United States the enforcer mentioned in the email is the IRS, while in the rest of the world it was that FATF. The third question asks, does offering more money for providers to violate the rules make them any more likely to do so? In brief the answers are not really, partly, and yes.

Perhaps surprisingly, there was little difference in the benchmark Dodgy Shopping Count (the Placebo rate was 11.5 in international sample, 9 in U.S. sample) in response to more information about the rules (DSC 11.2 internationally, 10.2 in U.S.). And the prospect of penalties for non-compliance from the FATF (13.2 internationally) did not significantly alter the Non-Compliance rate nor the Dodgy Shopping Count from which it is derived. However, the prospect of enforcement by the IRS did significantly decrease the Non-Compliance rate in the United States, which thus boosts the Dodgy Shopping Count from 9.5 in the Placebo to 13.2 for the IRS condition. The significance of the first finding is that it is not ignorance that causes non-

compliance globally. The IRS, however, seems to better get the attention of would-be anonymous shell providers in the U.S. than the FATF internationally.

Offering providers in the international sample more money to break the rules made them less likely to be found Non-Compliant, boosting the Dodgy Shopping Count from 11.5 to 16.6, but this increase was not statistically significant. On the other hand, the Premium condition did cause a statistically significant decrease in the Compliance rate, dropping from 18.9 in the Placebo condition to 14.2 for the Premium treatment.

In combination, relatively little of this material is good news in terms of the effectiveness of rules that are meant to govern shell companies. Untraceable shell companies are in practice widely available. Despite their regular pronouncements to the contrary, rich, developed countries are delinquent in enforcing the rules on corporate transparency, doing significantly worse than developing countries, and three times worse than the oft-reviled tax havens. Even customers who should be obvious corruption and terrorism financing risks to any provider exhibiting any risk-sensitivity are still regularly offered untraceable shell companies. Providers are relatively indifferent to coaching and the prospect of penalties from the global regulator FATF (but are more responsive to the IRS in the United States), and a significant proportion can be bribed to flout international rules.

A final point in explaining the results relates to non-responses. Internationally, 49.3 percent of the email approaches sent out did not receive a reply. In the United States sample the proportion of non-responses was even higher at 77.3 percent, while among law firms in the U.S. sample it reached 83 percent. What does this substantial proportion of non-responses mean for our results? Potentially, these non-responses could be a form of "soft compliance": if a provider judges a potential customer to be too suspicious the provider might decide that the best response is none at all. If this were generally true, it would indicate that the system works much better than we suggest, because most or all of the non-responses could be judged as evidence of the rules working. The suspicious customer does not get an untraceable shell company (or any shell company at all). On the other hand, if non-responses have nothing to do with *de facto* risk screening, and are just a product of commercial decisions, uninterest or disorganization, then non-responses cannot be regarded as evidence of the system working.

Our evidence suggests that the latter situation is more likely, and that a large majority of non-responses do not reflect customer risk. To test this we sent a brief, no-risk follow-up email to all those providers who did not respond, using a different Norstralia alias and simply 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 United States did not respond to this most innocuous inquiry, indicating that customer risk had little to do with their silence.

Legality and Ethics

Before concluding the paper, it is important to clarify that the project has not involved breaking any laws. Also, the study obtained ethical clearance from the governing Institutional Review Board (IRB).

First, the project was based on soliciting offers for shell companies, but we did not buy any shell companies (a much smaller earlier study did).[29] None of the names we used was real, and signing any legal documents in these false names would have been a criminal offence. When the providers responded with what identity documents were required (if any), we responded with an email thanking them for their time and telling them that our business needs had been met.

Given that the project was based on impersonating fictitious characters and pretending to be interested in buying shell companies, it was based on deception. Indeed, this deception gives us confidence that we did receive genuine answers from providers. But deception must be ethically justified. In line with general principles governing such research, deception can only be justified where (1) the costs are low, (2) subjects are not exposed to any physical or emotional pain, (3) there is no other way to do the research, and (4) there are significant benefits resulting from the research.[30]

We estimate that providers took 3-5 minutes to respond to our emails, so costs were minimal. Since our approaches closely mirror the day-to-day business of subject firms, there was no harm inflicted. We destroyed all identifying information on individuals and individual firms to ensure that none can be penalized for the responses they gave. We could not have found out the availability of untraceable shell companies without deception. Directly asking people or firms if they follow rules is not a reliable way of finding out whether they really do follow such rules in practice, especially if they routinely behave inappropriately. Shell companies are a major factor behind criminal successes and all the associated human suffering. Better knowledge on the effectiveness of existing policies on shell companies should help improve these policies and reduce the harm caused by crime. The potential benefits of the research are therefore significant.

Conclusion

As noted at the outset, organized crime and terrorism depend on financial secrecy. Untraceable shell companies are the most important means of providing this financial secrecy. Recognizing this danger, the international community has responded by mandating that authorities must be able to look through the corporate veil to find the real individuals in control of shell companies. Yet until now, no one has known how effective these policy measures have been. Our study goes a long way to remedy this fundamental ignorance. By identifying the serious weaknesses in the existing regime we hope to provoke governments to much greater efforts in enforcing corporate transparency.

1. Michael Findley is an Assistant Professor at the Department of Government at the University of Texas, Austin. mikefindley@austin.utexas.edu

2. Daniel Nielson is an Associate Professor and Director of the Political Economy Development Lab at Brigham Young University. dan_nielson@byu.edu

3. Jason Sharman is a Professor and Director of the Centre for Governance and Public Policy, Griffith University, Australia. j.sharman@griffith.edu.au

1 This report provides a basic summary of the main findings. Further information will be available in published work or upon request.

2 Kevin McCoy, "Project Shows Ease of Money Laundering in USA," USA Today, 19 March 2007 http://www.usatoday.com/money/companies/2007-03-19-money-launder-usat_N.htm; J.C. Sharman, The Money Laundry: Regulating Criminal Finance in the Global Economy (Ithaca: Cornell University Press, 2011); Emile van der Does de Willebois, Emily Halter, Robert A. Harrison, J.C. Sharman and Ji Won, The Puppet Masters: How the Corrupt Use Legal Structures to Hide their Stolen Assets and What to do About It (Washington D.C.: World Bank, 2011); National Public Radio "We Set Up an Offshore Company in a Tax Haven," 27 July 2012 http://www.npr.org/blogs/money/2012/07/27/157421340/how-to-set-up-an-offshore-company.

3 OECD, Behind the Corporate Veil: Using Corporate Entities for Illicit Purposes, Paris, 2001.

4 "North Korea Weapons Plane 'Was Heading to Iran'" Times, 21 December 2009

5 Jo Becker, "Web of Shell Companies Veils Trade by Iran's Ships," New York Times, 7 June 2010.

6 United States District Court for the District of Columbia, United States of America versus BAE Systems plc, Criminal No. 1:10-cr-035, 22 February 2010.

7 US Senate Permanent Subcommittee on Investigations, Keeping Foreign Corruption out of the United States: Four Case Histories, Washington D.C., 2010.

8 http://russian-untouchables.com/

9 United States District Court Southern District of New York, United States of American versus Wegelin & Co., Michael Berlinka, Urs Frei and Roger Keller, Indictment S1 12 cr.02 (JSR), 2011.

10 Sen. Carl Levin New Release "Levin, Grassley Introduce Bill to Combat U.S. Corporations with Hidden Owners," 2 August 2011.

11 Fintrac (Canada), Money Laundering and Terrorist Activity Financing Watch, January-March 2010, available at http://www.fintrac.gc.ca/publications/watch-regard/2010-09-eng.pdf.

12 US Senate Permanent Subcommittee on Investigations, Tax Haven Abuses: The Enablers, The Tools, and Secrecy, Washington D.C., 2006; US Senate Permanent Subcommittee on Investigations, Keeping Foreign Corruption out of the United States, 2010; Jack Blum, Michael Levi, R. Thomas Naylor, and Phil Williams. Financial Havens, Banking Secrecy, and Money Laundering. Vienna: United Nations Office for Drug Control and Crime Prevention, 1998; European Commission. Euroshore: Protecting the EU Financial System from the Exploitation of Financial Centers and Offshore Facilities by Organized Crime, Trento, 2000; FATF, The Misuse of Corporate Vehicles, Including Trust and Corporate Service Providers. Paris, 2006; Van der Does de Willebois et al., The Puppet Masters, 2011; Global Witness. Undue Diligence: How Banks do Business with Corrupt Regimes. London, 2009; Global Witness, Grave Secrecy: How a Dead Man can Own a UK Company and Other Hair-Raising Stories about Hidden Company Ownerships from Kyrgyzstan and Beyond, London, 2012.

13 FATF, The Misuse of Corporate Vehicles, 2006.

14 Economist "The Incorporation Business: They Sell Sea Shells," 7 April 2012; Economist "Shells and Shelves," 7 April 2012.

15 FATF Recommendation 24, see FATF, International Standards on Money Laundering and the Financing of Terrorism & Proliferation, 2012: 24 available at http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%20%28approved%20February%202012%29%20reprint%20May%202012%20web%20version.pdf

16 For example, the G20 summit in Pittsburg called upon "the FATF to help detect and deter the proceeds of corruption by prioritizing work to strengthen standards on customer due diligence, beneficial ownership and transparency." http://www.g20.utoronto.ca/2009/2009communique0925.html#system, paragraph 42.

17 OECD, Behind the Corporate Veil, 2001.

18 van der Does de Willebois et al., The Puppet Masters, 2011.

19 The only exception is in the country-by-country league table. In that one, we pool the results together to provide a fuller picture.

20 Richard Gordon, Laundering the Proceeds of Public Sector Corruption: A Preliminary Report. Washington D.C., World Bank, 2009; Sharman, The Money Laundry, 2011; Van der Does de Willebois et al., The Puppet Masters, 2011.

21 We created fictitious firm names here for illustration purposes and to avoid identification of any actual companies used in the experiment.

22 These countries are all in the lowest quintile of Transparency International's Corruption Perceptions Index, see http://cpi.transparency.org/cpi2011/results/

23 FATF, International Standards, 2012, 63.

24 OECD, Bribery in Public Procurement: Methods, Actors and Counter-Measures, Paris, 2007.

25 Robert A. Pape, Dying to Win. New York: Random House, 2005.

26 FATF, International Standards, 2012, 54.

27 FATF, Risk-Based Approach: Guidance for Trust and Company Service Providers, Paris, 2008: 22.

28 We verified the balance through a variety of randomization checks that looked to see if factors such as the type of base country or firm were evenly distributed across conditions. We encountered very few imbalances, and in these few cases we employed statistical fixes by adding control variables. None of the fixes meaningfully changed the results we report here.

29 J.C. Sharman, "Shopping for Anonymous Shell Companies: An Audit Study of Financial Anonymity and Crime," Journal of Economic Perspectives 24 (Fall 2010), 127-140.

30 Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects Research. 1979. Department of Health, Education, and Welfare. Online at: http://ohsr.od.nih.gov/guidelines/belmont.html.