The Real Danger Behind the Offshore Business:
Identity Laundering

Marius Burcă
Valahia University, Târgovişte, Romania

Every once in a while the public is presented with new evidence that offshore business is evil. The Panama Papers make the latest example. This research would like to expose that offshore business is incriminated for the wrong reasons. Although it may be more popular to call upon the collective empathy that all equal people should equally pay their due tax, the author would like to back the idea that it is not money laundering (and, implicitly, tax evasion), but the terrorist financing which poses the real threat to modern day mankind. The true vulnerability is that the ultimate beneficial owner of any assets managed in offshore companies is no longer visible, which creates the perfect nest for nurturing terrorism. Offshore is not only tax haven, but could also easily become financing terror haven. The solution resides in enforcing ID laundering controls, based on the anti-money laundering ones, such as “Know Your Customer”, on a global scale. The challenges are related to how we all shape the present day definitions of privacy, freedom, and ultimately, human rights.

Keywords: offshore, shell companies, terrorism financing, money laundering, ID laundering, tax havens

On April 3, 2016, people from around the world were made aware of the “The Panama Papers”, a set of confidential documents which show how wealthy and influential people, including public officials, have concealed their assets away from the regulators in their home countries. A Panama-based law firm allegedly created about 214,000 shell companies from 1977 through the end of 2015, in various offshore jurisdictions around the world, such as the British Virgin Islands, Panama, Bermuda, Seychelles as well as other territories which offer significant tax benefits to foreign capital (BBC News, 2016b; The Independent, 2016b).

According to Wikipedia.org the leak dates back to the early 2015 when an anonymous source made the documents available in batches to the German newspaper “Süddeutsche Zeitung”. The information from this “unremunerated whistleblower” eventually totaled 2.6 terabytes of data (11.5 million documents referring to 214,488 offshore entities linked to 14,153 clients in 200 countries and territories).

Given the scale of the leak, the newspaper enlisted the help of the International Consortium of Investigative Journalists (ICIJ), which distributed the documents for investigation and analysis to some 400 journalists at 107 media organizations in 76 countries. The ICIJ plans to publish a full list of companies involved in early May 2016. (Wikipedia, 2016a)

The disclosure has raised waves of mass emotions all around the world (Wikipedia, 2016b). The Icelandic Prime Minister “stepped aside for an unspecified amount of time” (Iceland Monitor, 2016) after facing serious anti-government protests outside the Parliament from over 20,000 people, which made Edward Snowden [former

Corresponding author: Marius Burcă, Ph.D. researcher, Valahia University, Târgovişte, Romania; research fields: management, human resources, anti-fraud and anti-money laundering in e-commerce (online gaming).
Central Intelligence Agency (CIA) employee who leaked classified information from the National Security Agency (NSA) on numerous global surveillance programs—https://en.wikipedia.org/wiki/Edward_Snowden—wonder whether that would be “the largest protest by percentage of population in history” (Snowden, 2016).

The UK Prime Minister David Cameron had found himself in an awkward position when he received political pressure to take action in respect to enforcing more control over British overseas tax havens whilst the Panama Papers revealed his family’s close links to “tax avoidance” (The Independent, 2016a).

The world is still undecided whether “tax avoidance” is actually not yet incriminated “tax evasion” which is acted via the offshore businesses. Although there is no formal definition, a jurisdiction is considered an “offshore financial center” (less formally known as “tax haven”) when their banking infrastructure:

1. Focuses on providing services to non-residents;
2. Requires little or no disclosure of business information;
3. Offers low or zero tax scheme (Zoromé, 2007).

Doing business in such a jurisdiction is not illegal per se, and not even morally wrong (Australian Broadcasting Corporation, 2016).

However, the journalists and researchers such as “The Economist” and the “Tax Justice Network” concluded that “The most obvious use of offshore financial centers is to avoid taxes” (The Economist, 2007; Harari, Meinzer, & Murphy, 2012).

Furthermore, Igor Angelini, head of Europol’s Financial Intelligence Group, said that the shell companies used for this purpose “play an important role in large-scale money laundering activities” and that they are often a means to “transfer bribe money” (Leyendecker, Obermaier, Oermayer, & Wormer, 2016).

**Tax Havens Dilemma**

Based on the above, there seems to be efforts to have crowds convinced that offshore business could be evil because it may facilitate money laundering. The author of this paper would like to express different views, as follows:

1. Although the modern international regulations are incriminating it as a separate offence, money laundering, by its mechanics, is not a crime in itself (Angell, 2016) but an alert to a probable underlying fraud (predicate offence). The said elusive prime crime had been committed within the home jurisdiction, and not the offshore one. When a public official from a certain country where they live and work receives bribe money into an offshore account, the bribe constitutes the proceeds of corruption undergoing within the public official’s home country, so the whole illegal activity was executed by residents of that particular jurisdiction. Therefore, there seems to be issues with crime prevention and deterrence in the home jurisdiction, and not in the offshore one. Most of the times, we come to know hidden things by their effects, and therefore we should take action on the cause rather than on the effects. Banning the offshore business (the effects) will not combat fraud (the cause). Instead, it will rather prevent us from using this tool to see the underworld of crime. Furthermore, shutting down one exit point will only push crime to find other ways out, and not necessarily those where justice could be easily enforced;

2. What it is deemed legal or illegal changes from time to time and from jurisdiction to jurisdiction. Therefore, it is not the offshore regulation which should filter and only allow lawful activities in different territories or across time, but the home regulations should install adequate controls to fight crime within their legal reach;
(3) The real threat, though, when using shell companies is that the ultimate beneficial owner may not be transparent, since the offshore regulations do not require detailed disclosure of business activities. The reason for non-disclosure may be related to global market pressure and competitiveness: If not for obvious advantages lacking at home, why would anyone bother registering companies and doing business in remote locations? However, regardless of the stiff competition, nothing should justify crime.

An interim conclusion is that tax havens are not intrinsically bad. There are known regions even within prominent countries (including the US—Nevada, Delaware etc., and China—Special Economic Zones) which enjoy tax or other benefits in order to support local development. The same logic of supporting local communities was applied when small and remote locations (mostly tiny islands) started to offer impressive tax and non-disclosure benefits to foreign investors. However, those facilities may be misused for crime and although money laundering is the tip of the iceberg for deeper illegal activities, still the most important threat of the offshore benefit misappropriation would be concealing of the true identity of the real owners of the capital managed by the shell companies.

Therefore, many experts believe that the current legal system needs improvements. Shruti Shah, Vice President of the Transparency International-USA, remarked:

(…) it is absolutely legal in many parts of the world to form a company without disclosing who the true beneficial owner is, including right here in the United States. In every state in the U.S., you can form a company without having to disclose who the person is that really controls the company or derives economic benefit from it. And also here, you know, people, gatekeepers such as real estate agents and others, don’t have to do any due diligence on buyers’ identities or the sources of their funds. So, what he has pointed out is really the crux of the problem. The structure needs reform. (PBS NewsHour, 2016)

In Europe, the five largest economies in the European Union have agreed to share information on secret owners of businesses and trusts (BBC News, 2016a).

Consequently, according to the above cited source, information on the ultimate beneficial owners will be automatically exchanged among authorities in the UK, France, Spain, Italy, and Germany. Those countries will push the rest of G20 members to follow suit—which means data exchange on previously secret tax information among countries such as the US, Saudi Arabia, and China.

Those European actions are not entirely new, but follow a trend set by the European Union Directives, such as the Directive 849/215, or better known as “The Fourth Anti-Money Laundering Directive” (EUR-Lex, 2015).

One of the novelties introduced by the above mentioned directive is the implementation of a centralized and common registry where the information of the ultimate beneficial owners of the companies registered within the European Union is transparent and publicly available. There are also voices which support the idea that the UK should enforce similar actions on the crowns’ dependencies (CCH Daily, 2016).

Those efforts on increased transparency are definitely a good step forward. However, the author of this paper would like to point out that:

Fighting a large spectrum of crime in one shot is good, but not good enough. Right now, we are told that offshore regimes could harbor money laundering related to different underlying offenses like tax evasion, corruption, human trafficking, or illegal drug and weapon trade. This is true but incomplete: The real vulnerability of the offshore is the risk of Identity (ID) Laundering, with very serious consequences like facilitating the financing of terrorism.
Therefore, we need specific measures to prevent, deter, and combat ID Laundering.

**ID Laundering**

The author believes that ID Laundering is performed by any shell company who disguises the true and real beneficiaries and directors of certain businesses. Any official of a shell company who is acting on behalf of an undisclosed individual is doing ID Laundering. To extend it further, any person in the world who is acting on behalf of someone else, without revealing his being an agent and with keeping the identity of the beneficiary concealed, is doing ID Laundering.

ID Laundering could be a perfectly legal operation if some beneficiaries choose discretion only. However, one might observe the level of the said discretion so that no innocent person should be shy of disclosing full financial data to relevant authorities. Hence, ID Laundering is not a crime, but an alert which should trigger further investigation.

When performing ID Laundering, the true beneficial owner in the shadow could simply be anybody, including the terror organizations. As those terror groups fight a global war with no rules, practically anyone in the world (including children) could become a victim at any given time. This risk is by all means not acceptable and should be more seriously mitigated by controlling the ID Laundering.

The tools to deal with ID Laundering should be adapted from those of combating money laundering, i.e. Customer Due Diligence (or better known as Know Your Customer), which mainly means:

1. The verification of customers’ identity based on documents released by authorities or other independent and trust worthy institutions;
2. The identification of the beneficial owner;
3. The assessing (on a risk-based approach) and the understanding of the purpose and intended nature of the business relationship, including, where necessary, the source of funds;

**Mitigating the Risk of ID Laundering**

The risk of ID Laundering could be mitigated when all companies perform the following verification of their customers:

1. Identify who the ultimate and real beneficial owner is;
2. Understand the customer’s source of funds.

If the customers are legal entities, then the ID Laundering verification should be attempted on the owners of those companies, most specifically on those whose stakes are 25% or higher. If the stakeholders are in turn legal entities, the process is repeated until the ultimate beneficial owner is a private individual.

If the customers are private individuals, in many cases those are the real beneficial owners. However, there could also be instances when private individuals are mere agents acting on behalf of other undisclosed individuals, and they do not even reveal their being agents. As stated above in this paper, this is considered ID Laundering and although not a crime in itself, any suspicions of ID Laundering should trigger further investigations related to the identity of beneficial owners as well as to their source of funds.

The problem with enforcing the ID Laundering controls on a world-wide scale (in order to become efficient) is that the parent of ID Laundering, i.e. Anti-Money Laundering Regulations, regardless of the issuing
jurisdiction, apply to certain types of organizations only (the obliged entities) and usually include credit and financial institutions, tax advisers, notaries, real estate agents, and providers of gambling activities. All the other businesses are not required to comply, unless they deal with suspicious transactions over certain threshold. Modern day fraudsters and terrorists always find ways to stay below the threshold and avoid being suspicious, and therefore the author of this paper suggests that regulations world-wide should include the ID Laundering controls for all businesses.

Establishing business relationships with shell companies should not be restricted by law—Just the verifications should be performed more thoroughly. If the offshore company officials are hostile in revealing the true identity of the beneficial owners and the source of funds, then a cross-check examination should be performed. Some key leads to follow could be whether the shell company’s officials hold similar positions in other offshore companies, if the registered office is shared with other companies, whether the source of funds appears legitimate and proportionate with the business activity, and so on. The results of those checks may become red flags for ID Laundering which could cover deeper illegal activities, and therefore the suspicious activity should be reported to relevant authorities. It is advisable that business relationships should discontinue until further clarifications are reached.

Conclusions and Implications of Installing ID Laundering Controls

There is absolutely no doubt that, by their tax and non-disclosure benefits, the offshore jurisdictions may be misused for money laundering. The underground economy, corruption, and tax evasion prevent communities from proper development and negatively impact their members’ welfare, which could become, in some instances, even life threat. However, money laundering and its associated underlying offences affect us indirectly, whereas when a bomb blows up in a crowded location, anytime, anywhere in the world, it is affecting our lives very directly. The risk of terrorism should be mitigated seriously before it metastasizes world-wide. The ID Laundering controls make, by the author of this paper, the right tools for combating terrorist financing.

Yet, there is always a thin line with respect to the legal grounds of investigations: People do not need to prove they are innocent; instead, the prosecutors need to gather evidence and the courts will decide whether anyone is guilty or not. The gathering of evidence may conflict with the privacy rights, with how modern people see freedom and, ultimately with the basic human rights where anyone should be given the benefit of the doubt.

A possible solution would be the wide implementation of the integrated money laundering and ID Laundering controls into everybody’s life. People will eventually see it as part of the today’s life, preserving the common good and deterring criminal behaviour. Apart from those in the airports which are now simply part of the journey, the increasing security checks in many museums, train stations, and other popular and crowded places will eventually shape the new definitions of privacy and freedom.

References