Illicit Finance and Money Laundering Trends in Eurasia

Abstract: This paper reviews recent examples of sophisticated money laundering operations involving financial institutions in Eurasia – including Russia and Moldova – and the resulting flow of licit and illicit capital from that part of the world to the UK, the US, and other Western countries. Relying on materials from publicly-available sources, it uses several case studies to illustrate various money laundering methods with a view toward identifying common elements and aspects of the schemes that might be considered new or innovative. In particular, the paper examines the roles that lax anti-money laundering (AML) compliance by financial institutions and the use of shell corporations designed to conceal the beneficial ownership of the companies and their assets have played in virtually all of the money laundering schemes. The paper then discusses the risks that these emerging money laundering methods pose to Western countries and their financial institutions and the approaches that governments might take to minimize those risks and to raise the barriers to the laundering of illicit funds within their jurisdictions.

I. INTRODUCTION

This paper reviews recent examples of sophisticated money laundering operations involving financial institutions in Eurasia – including Russia and Moldova – and the resulting flow of licit and illicit capital from that part of the world to the UK, the US, and other Western countries. Relying on materials from publicly-available sources, it uses several case studies to illustrate various money laundering methods with a view toward identifying common elements and aspects of the schemes that might be considered new or innovative.

In particular, the paper examines the roles that lax anti-money laundering (AML) compliance by financial institutions and the use of shell corporations designed to conceal the beneficial ownership of the companies and their assets have played in virtually all of the money laundering schemes.

The paper then discusses the risks that these emerging money laundering methods pose to Western countries and their financial institutions and the approaches that governments might take to minimize those risks and to raise the barriers to the laundering of illicit funds within their jurisdictions.

II. CASE STUDIES

A. The Russian Laundromat

"The Russian Laundromat" is the term given by the media to a scheme for laundering the proceeds of Russian criminal activity through shell corporations and European banks that flourished from 2010 to 2014. While the operation has been shut down, it serves as an illustration of the vulnerabilities of the Western financial system to a money laundering operation centered in places where AML controls are lax, and corruption is common.

How it worked

Russian businesses controlled by oligarchs with ties to the Russian state and to Russian organized crime amassed billions of dollars in illicit proceeds in Russian banks, and needed a means of creating the appearance that the money came from a legitimate source. According to media reports, the money was derived from a variety of illegal sources, including contract fraud (*i.e.,* inflated payments on contracts with the Russian state), tax evasion and tax fraud, embezzlement from Russian banks and other corporations, and generic organized crime (drug trafficking, human trafficking, etc.).[1]

To launder the money, a Russian business holding criminal proceeds would create two shell corporations and paperwork that made it appear that one of those corporations owed money to the other. The Russian business would then guarantee the "debt," so that when one of the shell corporations "defaulted" on the "loan" to the other, the Russian business would be liable to pay it.

Each of the Russian businesses included a Moldovan citizen as a responsible party so that when the "default" occurred, the shell corporation seeking payment could resort to the Moldovan courts. With the cooperation of corrupt Moldovan judges, the shell corporation would obtain a court order directing the Russian business to pay the debt to an account at a Moldovan bank. Complying with the court order, the Russian business would transfer the criminal proceeds being laundered to the Moldovan bank, at which point the shell corporation receiving the money was free to disburse it anywhere in the world to pay for whatever assets the beneficial owners of the shell corporation wished to acquire.

The following diagram illustrates the process:

Because the money was deposited into the Moldovan bank pursuant to a court order, it acquired the appearance of legitimacy, and because the ownership of the shell corporations was not disclosed (either to the Moldovan bank or to the banks to which it transferred funds), the transactions provided a degree of anonymity to the persons conducting the transactions.

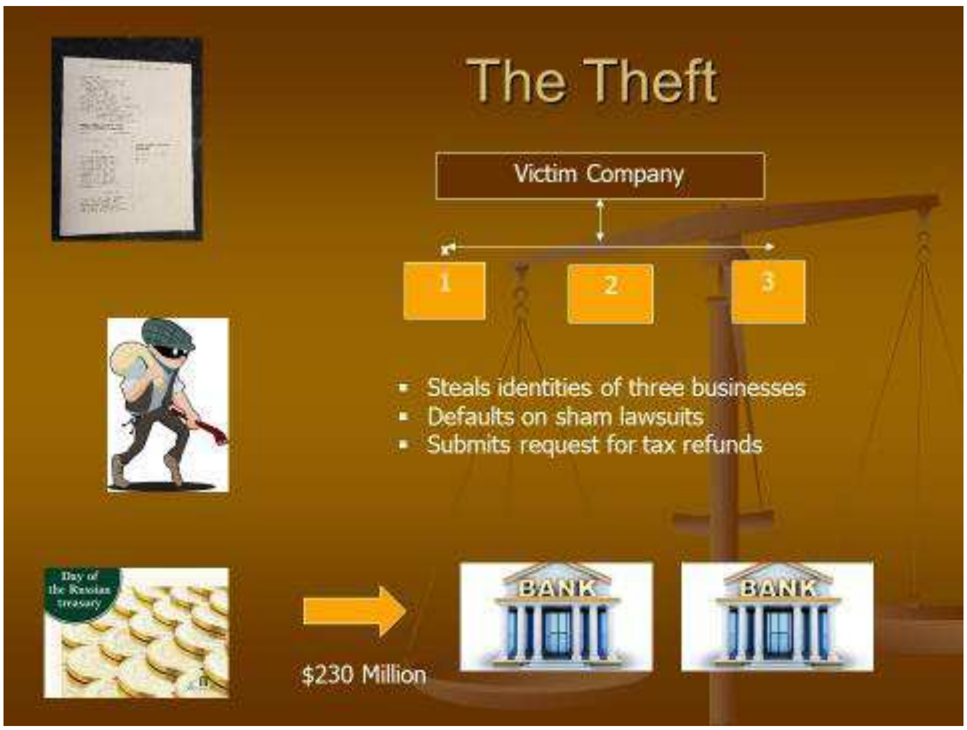
According to the media reports, at least US$20.8 billion was laundered in this fashion, and was used to make investments, purchase luxury items, and acquire merchandise imported by Russian companies from Western sources. In many cases, the success of the scheme depended on the willingness of the vendor of the goods and services to receive payment not from the purchaser directly but from a company based in a secrecy jurisdiction whose beneficial ownership was unknown to the vendor or to the bank processing the payment on the vendor's behalf.

B. The *Prevezon* Case

Closely related to the Russian Laundromat scheme, but occurring several years earlier, was the theft of $230 million from the Russian state through a tax fraud scheme, the laundering of that money through shell corporations with accounts at a Moldovan bank, and the investment of the money in real estate in New York. The case has earned some notoriety following the murder while in custody of Sergei Magnitsky, the attorney retained by one of the victim companies to investigate the fraud scheme.

As alleged in the civil action filed by the United States in the Southern District of New York, a Russian criminal organization stole the identities of three legitimate Russian companies by stealing corporate documents, and used the stolen identities to obtain undeserved tax refunds totaling $230 million from the Russian Treasury. To do so, the criminals orchestrated a series of sham lawsuits against the stolen companies, obtained default judgments against them, and used those judgments to obtain the tax refunds by claiming that the losses so reduced the companies' profits as to negate their tax liability.

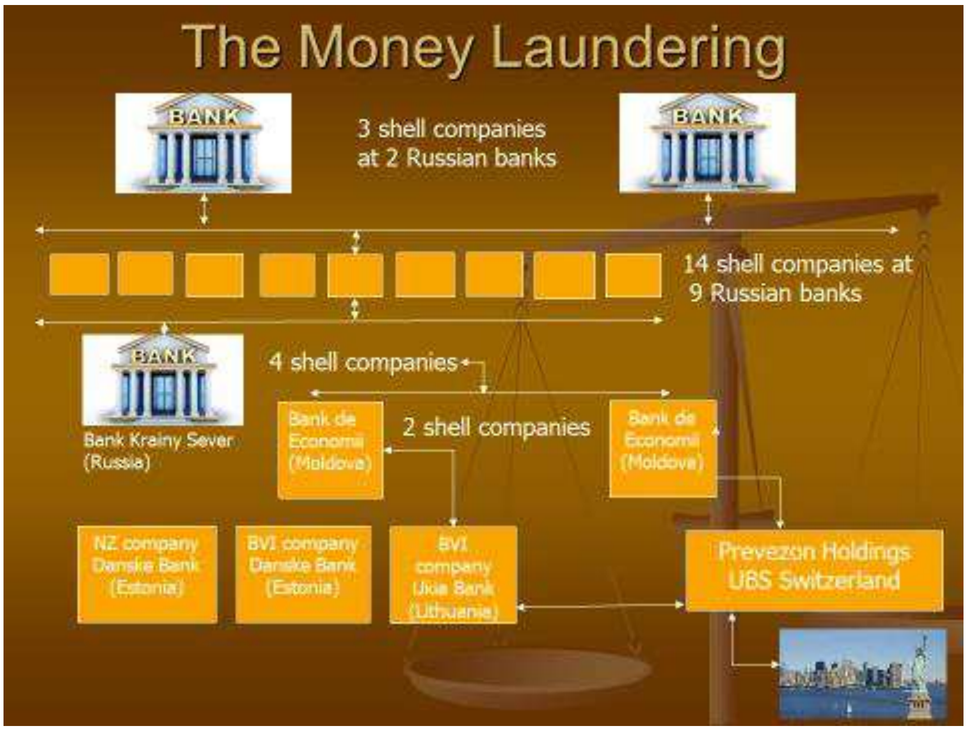
The following diagram illustrates how the fraud scheme was perpetrated and how it resulted in the deposit of $230 million in stolen funds into bank accounts controlled by the criminal organization.



The civil forfeiture complaint further described "a Byzantine web of conduit accounts" whereby the stolen money was transferred through no fewer than 14 shell companies at nine different Russian banks, was deposited in the correspondent account of yet another Russian bank for the benefit of four more shell companies, and ultimately was placed in the accounts of two Moldovan shell corporations at Banca di Economii in Moldova – all within a period of 60 days.[2]

Finally, part of the money, commingled with other funds, was transferred from the Moldovan companies to three entities: a New Zealand shell company and a British Virgin Islands shell company that had accounts at an Estonian bank, and another BVI company with an account at a Lithuanian bank. Finally, $1.9 million was transferred from the Moldovan and Lithuanian banks to the Swiss bank account of Prevezon Holdings, which used a portion of it to acquire a number of valuable parcels of property in Manhattan.[3]

The following diagram illustrates, in simplified form, the money laundering process.



On May 15, 2017, the acting U.S. Attorney for the Southern District of New York announced the settlement of this case, with the claimant agreeing to pay a civil penalty under 18 U.S.C. § 1956(b) of $5.8 million, which is three times the value of the property in NY that was involved in the money laundering offense.[4]

C. Moldovan Bank Embezzlement

Another case involving banks in Moldova was an embezzlement scheme whereby a small group of related entities controlled by Ilan Shor, a Moldovan businessman and politician, was able to extract $1 billion from three Moldovan banks, causing their collapse.

According to publicly-available sources, between 2012 and 2014 Shor and individuals associated with him were able to gain a significant shareholder interest in Banca de Economii, Unibank and Banca Socială, financing their acquisitions with loans from offshore companies, each with Latvian bank accounts. Shor was then able to engineer a series of loans from the three banks to entities that he and his associates controlled, using loans from one bank to service the debts owed to another until ultimately he had obtained a loan of MDL13.8 billion (US$1 billion) which was not repaid. The three banks collapsed in 2014 and had to be bailed out by the National Bank of Moldova.[5]

The US$1 billion in loan proceeds was disbursed to entities incorporated in the UK and Hong Kong with bank accounts in Latvia.[6] The money, which represents one-eighth of the annual GDP of Moldova, has not been recovered. One defendant, Veaceslav Platon, who was also implicated in the Russian Laundromat scheme, was convicted in April 2017 and ordered to pay US$45 million in damages. Former Moldovan Prime Minister Vlad Filat has also been convicted in connection with the embezzlement scheme.

D. The Kabul Bank Case

The facts of the Moldovan bank embezzlement scheme bear a striking resemblance to the embezzlement that caused the loss of $900 million and eventual near-collapse of Kabul Bank in Afghanistan in 2010. In that case, 19 related parties were able to obtain nearly $900 million in loans from the bank and were not required to make repayments. The money represented between five and six percent of Afghanistan's GDP.[7]

Efforts to recover the money from accounts throughout the world, including the United States, have been largely unsuccessful. The loan proceeds were initially disbursed to accounts in Dubai, but because that country does not honor requests for bank records from foreign governments and law enforcement agencies, it has been impossible to trace the money through the international financial system.

E. "Mirror Trading"

"Mirror trading" is the name given to a method of moving large sums of money out of Russia and into Western countries by means of making parallel trades in securities. It was used to expatriate flight capital, engage in tax evasion, and (in all likelihood) to launder criminal proceeds.

How it worked

A broker representing two companies with common ownership – one in Russia and one elsewhere – would approach the trading desk at a major international bank such as Deutsche Bank and ask to make two more or less simultaneous trades. The Russian company, the broker would say, wants to buy a large quantity of stock in a publicly traded company for, say, $10 million, while the foreign company wants to sell an identical quantity of the same stock in a

Western country such as the UK for around the same price. Because the two trades are the mirror image of each other, this process is called "mirror trading." [8]

To process the trade, the trading desk in Moscow would handle the Buy Order with funds provided by the Russian company, while the corresponding trading desk in London (or wherever) would process the Sell Order, depositing the proceeds of the sale into whatever account in the UK or elsewhere that the broker or his client might designate. Typically such trades would be on the order of $10 million.

The following diagram illustrates the mirror trading process:

Mirror trades make no economic sense: even if the client could avoid selling the stock on the foreign exchange for less than the purchase price in Moscow (a loss that is hard to avoid), the client would suffer a loss merely from having to pay the commissions of the various intermediaries, including the international bank and the Russian broker. Because the purchase occurred in Russia and the sale occurred elsewhere, however, the effect of such trades was to move large sums of money out of Russian and into Western countries.

In the above example, the effect of the two trades would have been to move $10 million (minus the fees) from Russia to the UK or another Western country, and to convert it from rubles to pounds, euros or dollars. Between 2011 and 2015 when such trades at Deutsche Bank were discovered and discontinued, Deutsche Bank alone processed $10 billion in such trades.

Motives and Effects

The obvious motive for engaging in a mirror trade is to expatriate large sums of money from Russia to Western countries where it can be invested in "safe" assets, such as real property in London or New York. In many instances, the money is simply flight capital, and the purpose of the movement of the funds by wealthy individuals is simply to evade Russian income taxes and/or to place savings in more secure investments than are available in Russia. While the motive for such activity may be relatively benign, the effect of this form of money laundering is to weaken the Russian tax base and to raise the prices of Western assets, such as real property in London or New York.

There are more sophisticated (and perhaps more sinister) reasons for accepting the small loss associated with engaging in a mirror trade, however. A Russian importer, for example, might be seeking to evade Russian excise taxes by under-invoicing the quantities of goods being imported, and using the expatriated funds to pay his supplier for the additional goods that did not appear on the invoice. Or a Russian individual or entity might be seeking to evade the sanctions imposed on Russia by the US and the EU that have made transacting business in the West more difficult.

In those cases, as in pure flight capital cases, the money being moved out of Russia would have been legitimately derived. The same process, however, could be used to move *criminal proceeds* out of Russia to hide it from law enforcement, to use it to fund a luxurious lifestyle, or to finance terrorism or other criminal activity.

The failure of oversight by financial institutions

The apparent willingness of clients to lose money repeatedly on seemingly meaningless trades should have alerted the financial institutions such as Deutsche Bank that were handling the transactions that their clients were engaged in the expatriation of flight capital if not something more serious in nature. The employees at the trading desks who handled the trades on a day-to-day basis would also have been aware that the supposedly different clients engaged in the mirror trades were represented by the same broker and/or had overlapping or common ownership. Yet neither Deutsche Bank nor any of the other international banks processing mirror trades between 2011 and 2015 reported them to the appropriate authorities, or ceased making such trades on their own.

As discussed below, this may reflect nothing more than the inherent reluctance of banks to turn away business, or to alert law enforcement to suspicious activity, unless the particular financial activity appears on the list of things to watch out for and to report. That is why financial institutions are slow to react to new methods of money laundering. According to press reports, however, there may have been more direct complicity on the part of institutions such as Deutsche Bank in this instance, as one or more bank employees may have received bribes and gifts to allow the mirror trading to take place.

"Dark Matter"

The mirror trading process was likely just one part of a much larger movement of Russian capital to the West. According to a paper published in 2015, roughly 18 billion British pounds flows into the UK each year, a large portion of which represents Russian flight capital or criminal proceeds from Russian sources.[9] Moreover, the authors report that a large portion of the inflow of hidden capital enters the UK through the securities market, with the assets often held by shell companies whose beneficial owners are not known.[10]

F. Case Study: The Panama Papers

The disguising of the beneficial ownership of shell corporations has posed a problem for regulators, policy makers and law enforcement agencies for decades. The phenomenon is not new and was not previously unknown, but the scope of the use of shell corporations to disguise the beneficial ownership of assets on a global scale entered the public consciousness in a major way in 2016 with the disclosure of the documents known as the Panama Papers.

As numerous media reports have explained, the Panama Papers revealed that a Panamanian law firm, Mossack Fonseca, was responsible for creating a huge number of off-shore shell corporations that served the interests of a worldwide clientele. The corporations were formed in secrecy jurisdictions such as the British Virgin Islands by nominee directors whose names were the only ones that appeared on the corporate papers – thus providing anonymity to the actual beneficial owners of the companies and their assets.

That *someone* was forming shell corporations for the benefit of anonymous owners was not news; what was important was that the Panama Papers – documents leaked from Mossack Fonseca's electronic files -- revealed who the beneficial owners of many of those corporations actually were. Prominent persons, including political leaders in numerous countries, such as the Prime Minister of Iceland, were among those named.

According to press reports, Russian President Vladimir Putin and his circle of wealthy associates used Mossack Fonseca to create shell companies with names like Sandalwood Continental, Ltd, and International Media Overseas, and then used Russian banks that they controlled to "loan" billions of dollars to those companies. The companies, in turn, made more money by loaning the loan proceeds to other entities at high interest rates, or invested the money in assets in which Putin and his associates had an interest. It is unclear whether the loans were ever repaid.[11]

In short, the Panama Papers revealed that for some wealthy and politically-connected Russians, it was not necessary to go through the elaborate steps involved in mirror trading or the Russian Laundromat to move large sums of money overseas. It was necessary only to have control of a bank and access to the key ingredient in all of these schemes: off-shore shell corporations operating in jurisdictions that guaranteed the secrecy of the names of the beneficial owners.

III. COMMON ELEMENTS IN SUCCESSFUL MONEY LAUNDERING SCHEMES; IS ANY OF THIS NEW?

Money laundering is an ever-changing, dynamic process. It is a global game of whack-a-mole. Whenever regulators or law enforcement professionals identify one method of laundering – whether it be the "smurfing" operations of the 1980s or the advent of the Black Market Peso Exchange in the 1990s – and find ways to address it, the criminals and their associates find a new way to exploit the weaknesses and loopholes in the financial system – opportunities that rapid advances in technology are making available on a daily basis.

For that reason, it might seem pointless to focus too much on the creativity of a particularly innovative and successful but short-lived money laundering method: the old scheme, now that it has been uncovered, is probably no longer in operation, and another method, even more creative and complex, has probably already taken its place.

But that does not mean that Governments do not need to react to new money laundering schemes as they emerge. While it is true that a particular money laundering method – such as the Russian Laundromat or mirror trading – will inevitably be replaced by another method, the international money laundering schemes that have recently been uncovered do differ from what has been seen before in various ways that cause concern, including the speed which the money was moved, the volume of money that was moved in a short period of time, the level of corruption involved in the courts and the financial industry, the complexity of the schemes and the instruments used, and the value of the assets that the wrongdoers were ultimately able to acquire and maintain.

In short, as the case studies discussed above illustrate, advances in technology and globalization have increased the risks to which Western countries and their institutions are exposed, and have increased the magnitude of the harm that a successful money laundering operation can inflict in a short period of time.

This is, of course, part of a well-established pattern. As regulators develop new tools to detect wrongdoing and protect the integrity of institutions, and as law enforcement finds new ways of identifying perpetrators, imposing punishments, and recovering assets, technology offers money launderers still more innovative, faster, and ultimately more dangerous ways of moving illicit funds into the stream of commerce, and of disguising the purposes for which funds are being disbursed to far corners of the world. That is the lesson of the past four decades.

There is, unfortunately, an asymmetry to the process. Criminals and money launderers need obey no international borders; they need observe no rules of sovereignty or privacy; they are more nimble than governments in changing tactics; and they are always on offense, forcing regulators and law enforcement agencies to react, adjust, and catch up. Nevertheless, it is by reacting, adjusting and catching up with new money laundering methods as they emerge that Governments have managed consistently to raise the hurdles that wrongdoers confront, increasing their costs and their risks of exposure, and forcing them to operate in ever more inaccessible places or in less efficient and less convenient ways.

So governments must react; they must appreciate that the recently uncovered money laundering methods are indeed of a kind and magnitude not previously seen, and must respond by prosecuting the perpetrators, by seizing and forfeiting their assets, and by taking whatever steps are necessary to ensure that the gaps in the system that allowed these particular schemes to succeed are closed to future customers.

What is ultimately most important, however, is not to focus on the particular schemes that have been uncovered, but on their common elements – their basic components -- and to address them, knowing that those same components will likely form the core of the next money laundering method to be exploited and discovered. In short, it's not the details that matter; it's the common elements, the essential ingredients and the systemic weaknesses that allow new schemes to pop up whenever opportunity permits.

Common elements

A review of successful money laundering schemes like those discussed in the above case studies reveals several recurring, common elements that allow such schemes to flourish.

1. The use of shell companies formed in jurisdictions that do not require the identification of the beneficial owners of the companies or their assets.

2. Lax AML compliance by financial institutions (largely but not exclusively outside of the United States), and the inability or lack of motivation of such institutions to detect innovative ways of conducting transactions involving illicit funds. (Note: greater AML compliance in the US may be the reason why only $63 million of the money involved in the Russian Laundromat scheme found its way to the United States, and that a US bank was the only one to raise a money laundering concern.)

3. The lack of cooperation of financial institutions in bank secrecy jurisdictions with requests from the US and other developed countries for financial records.

4. Official corruption and the failure of bank regulators in developing countries to police self-lending within financial institutions. As the case studies demonstrate, official corruption (including corruption within the judiciary) facilitates lax enforcement of AML compliance programs and opens the door to the use of domestic financial institutions by foreign actors to launder the proceeds of foreign crime.

5. The willingness of vendors and their financial institutions to accept payments for goods and services from third parties with no apparent connection to the purchaser of the goods and services.

6. The inability of governments to recover criminal proceeds using existing tools that require strict tracing of assets to criminal activity, even as funds pass through secrecy jurisdictions and are invested in a succession of complex assets.

IV. RISKS TO WESTERN COUNTRIES

In addition to identifying the common elements of a successful money laundering scheme, policy makers should be aware of the risks that money laundering systems like those described in the case studies present to Western governments and their economies. Broadly stated, there are at least three principal concerns.

Surrendering the "high ground"

When financial institutions and providers of goods and services are used as conduits for, and recipients of, the proceeds of corruption, tax evasion, fraud, capital flight, and organized crime from the less developed parts of the world, or from places where corruption is endemic, they are wittingly or unwittingly facilitating criminal activity in the developing world and the diminution of the resources available in those countries to improve health, education, and infrastructure. No nation that aspires to a position of leadership on law enforcement issues – setting an example for others in the fight against the globalization of crime – wants to be perceived as the repository of the world's criminal proceeds, or as a facilitator of crimes committed at the expense of the impoverished citizens of the developing world. For that reason alone, the United States would be justified in taking all necessary steps to suppress the laundering of funds by, to, and through financial institutions in the US, and to recover and repatriate the property when it can be identified.

Prevention of new criminal activity

Second, a system that moves money through anonymous entities for the purpose of concealing the proceeds of past criminal acts can, once it is up and running, be used as easily to facilitate the commission of new crimes, such as financing terrorism, acquiring arms and explosive materials, and sending money to rogue states in contravention of international sanctions.[12] It is as important for nations to prevent the use of their financial systems to facilitate the commission of future criminal acts as it is to prevent them from being used to conceal the source or ownership of crimes that have already occurred.

Threats to national security and the integrity of institutions

Third, the infusion of criminal proceeds into a developed Western economy can provide criminals and criminal organizations with undue influence that may be used to corrupt public officials, influence the electoral process, or purchase controlling interests in important industries or real estate in major cities. Note, for example, that one of the perpetrators of the Russian Laundromat used millions of dollars laundered through Moldova to acquire shares in other Moldovan banks.

Allowing anonymous persons to acquire controlling interests in institutions, industries and physical assets presents a threat to the national security of the US and skews the economy in favor of persons with access to huge sums of untaxed cash to the detriment of would-be competitors in the marketplace who lack access to such resources.

V. RECOMMENDATIONS

Some aspects of commercial activity will inevitably lend themselves to exploitation by international money launderers. The huge volume of transactions occurring on a daily basis makes it difficult to analyze and investigate each transaction from the point of view of AML compliance, and the securities and commodities markets provide quick liquidity. Also, in many industries, such as securities trading and the provision of insurance products, the roles played by intermediaries – agents, brokers, lawyers and others – makes effective monitoring and enforcement difficult.

Policy makers also cannot ignore the facts of economic competition, domestically and globally: if increased AML compliance and awareness increases costs – costs that competitors choose not to bear and are able lawfully to avoid – it is unlikely that institutions vulnerable to money laundering will take on the additional costs necessary to make compliance effective.

Nevertheless, there are concrete steps that the United States and other governments could take to address at least some of the systemic weaknesses that have left them vulnerable to risks discussed above. For example, Western countries could:

1. Increase the awareness among vendors of goods and services, financial institutions, and other professionals, including attorneys, real estate agents, financial advisors, insurance agents and securities dealers, of the risks of accepting third-party payments, and of the existing consequences (including criminal prosecution and asset forfeiture) of knowingly accepting criminal proceeds in return even for legitimate goods and services.

2. Prohibit off-shore companies based in jurisdictions that protect the anonymity of their beneficial owners from moving funds through domestic financial institutions, acquiring fixed assets or significant interests in businesses, or paying for goods for export, without revealing the identities of the real parties in interest, and prohibit such companies from being formed in the United States. It is frankly embarrassing for the US to hold itself out as a leader in developing new ways of combatting international money laundering while taking virtually no steps to deal with the root problem – *viz.,* the of transparency in determining the beneficial ownership of business entities.

3. Make it a mandatory part of AML compliance for financial institutions to inquire as to the purpose of any transaction deemed to be unusual or suspicious, and to insist on evidentiary support for whatever explanation is given.

4. Similarly, make it part of the Know Your Customer requirement that financial institutions know when a customer is acting on behalf of a third party and who the third party is. For example, if a customer claims to be engaged in trade, the financial institution should know who the customer buys from and who it sells to; if it claims to be brokering a transaction between parties, the financial institution should insist on knowing who the counterparties are.

5. Insist that countries that seek the approval of their anti-money laundering legislation by the international community demonstrate not only that such legislation has been enacted, but that its law enforcement personnel have been trained to enforce the law and that enforcement actions have been successfully prosecuted.

6. Insist also that countries that seek access to US financial institutions on the part of their domestic institutions address systemic official corruption that threatens the integrity of their banks, their AML compliance programs, and their law enforcement actions.

7. Discourage "box ticking" compliance with AML programs by insisting that financial institutions train their personnel to do more than look for behavior known to have been indicative of money laundering in the past. While financial institutions are loathe to turn away business or scare away potential customers, their employees must be trained to be attentive to unusual conduct that seemingly has no economic purpose.

8. Provide law enforcement agencies with the resources to review and act upon Suspicious Activity Reports (SARs) and other information provided, formally or informally, by financial institutions. Resources should be sufficient to relieve federal law enforcement of the need to rely on detailees seconded from state and local agencies whose focus is necessarily on local crime (as opposed to complex international cases) and the recovery of assets that will inure to the benefit of the state or local agency.

9. Recognize that civil forfeiture is an indispensable tool of law enforcement in the international money laundering context, and that efforts to weaken it – such as by raising the burden of proof on the requirement that a given asset is traceable to an offense – would be injurious to the national interest. Criminal forfeiture is available only if the perpetrators of the crime can be apprehended, brought before a court in the US and convicted. Civil forfeiture, therefore, is the only vehicle for recovering assets when the perpetrators remain abroad. Current efforts in Congress to weaken civil forfeiture would accordingly have an enormously adverse effect on the Government's ability to recover assets in international cases.

---

[1] OCCRP, "The Russian Laundromat Exposed," March 20, 2017, https://www.occrp.org/en/laundromat/the-russian-laundromat-exposed; OCCRP, "The Russian Laundromat: The World Responds," March 28, 2017, https://www.occrp.org/en/laundromat/the-russian-laundromat-the-world-responds; L. Harding, et al., "British banks handled vast sums of laundered Russian money," The Guardian, March 20, 2017, https://www.theguardian.com/world/2017/mar/20/british-banks-handled-vast-sums-of-laundered-russian-money.

[2] *United States v. Prevezon Holdings, Ltd.*, 251 F. Supp.3d 684, 687 (S.D.N.Y. 2017).

[3] *United States v. Prevezon Holdings, Ltd.,* 2015 WL 4719786 (S.D.N.Y. Aug. 7, 2015), complaint available at https://ecf.nysd.uscourts.gov/doc1/127012958320.

[4] "Russian firm that promised to pay US millions after money-laundering settlement misses deadline," http://www.cnn.com/2017/11/02/world/russia-money-laundering-deadline-missed/index.html; "U.S. For First Time Defends Prevezon Money-Laundering Settlement," www.rferl.org/a/prevezon-settlement-money-laundering-u-s-defends/28915579.html.

[5] "Moldovan bank fraud scandal," Wikipedia, https://en.wikipedia.org/wiki/Moldovan_bank_fraud_scandal; Kroll Project, confidential report prepared for the National Bank of Moldova, provided to the public by Andrian Candu, speaker of the Moldovan Parliament, May 2015.

[6] Eurasian money launderers favor using bank accounts in Latvia because it is part of the European Union, which means that once funds are deposited in a Latvian bank, they can move freely throughout the EU and elsewhere.

[7] U.S. Special Inspector General for Afghanistan Reconstruction (SIGAR) Audit Report, January 2014, "Afghanistan's Banking Sector: Central Banks Ability to Regulate Commercial Banks Remains Weak" http://www.sigar.mil/pdf/audits/SIGAR%2014-16-AR.pdf

[8] This example is taken from Ed Caesar, "Deutsche Bank's $10-Billion Scandal," *The New Yorker,* August 29, 2016.

[9] Oliver Harvey and Robin Winkler, "Dark matter: the hidden capital flows that drive G10 exchange rates," (March 9, 2015), quoted in Caesar, supra.

[10] *Id.* at 9.

[11] *See* Luke Harding, "Revealed: the $2bn offshore trail that leads to Vladimir Putin," *The Guardian*, April 3, 2016, https://www.theguardian.com/new/2016/apr/03/.

[12] Some policy makers appear to be aware of this problem. For example, Rep. Sheila Jackson Lee (D-Tex.) has called for an investigation into whether the money stolen in the Moldovan bank embezzlement scheme was used to finance terrorism.