A gentle guide to money laundering

(Revised February 2020)

David Skillicorn,
School of Computing, Queen's University

Money laundering is the process of legitimising money obtained from illegal activities ('proceeds of crime'), moving it into the financial system in such a way that either it fails to attract the attention of authorities, or there is a plausible reason that can be used to explain its existence. The first mechanism is preferable because it also avoids liability for tax.

Much, although not all, illicit money is collected as cash, from activities such as drug sales, theft, and ransoms. It is possible to keep this as cash and spend it within a cash environment, but this is limiting to the owner mostly because it is dangerous to spend it in large amounts. Law enforcement have long used the tactic of watching for people who spend more than they legitimately earn. National tax authorities also watch for spending that is greater than declared income. Until relatively recently, many countries imposed a wall between their tax departments and their law enforcement to encourage criminals to declare, and pay tax on, the proceeds of crime. Famously Al Capone was prosecuted for tax crimes, not organised crime. Thus it is natural the criminals want to find ways to take cash and convert it into explained resources in the mainstream financial system. Once in the financial system, opportunities for moving it around, and so blurring the trail, are much greater.

National money laundering

We begin by considering money laundering in a national context, that is within a single country. It is still possible to buy expensive assets for cash, although opportunities are diminishing. Some of these assets are attractive because they are easy to transfer without any record (e.g. jewelry) so the eventual holder of such an asset cannot be linked back to the individual who bought it. In some Western countries it is still possible to buy a property worth millions and walk into the real-estate broker's office with the purchase price in cash. However, even in these countries this probably requires some level of collusion or wilful blindness on the part of the real-estate broker. Many jurisdictions have begun to push 'know your customer' regulations out to any profession that handles large amounts of money, requiring them to report large cash transactions. The opportunities for directly converting cash into valuable items are shrinking.

The other way to legitimise cash in a single-country setting is to leverage a suitable business. The best businesses are those where the gap between inputs (costs of raw materials) and outputs (prices charged) is large. For example, a pizza business may sell 1000 pizzas a month but buy the raw ingredients for 5000 pizzas a month, flushing the unneeded ingredients away. The cost of the discarded raw ingredients is much lower than the price of finished pizzas. The cash to be laundered is accounted for as cash purchases of the non-existent pizzas, and so becomes part of the apparently legitimate profits of the business. It is difficult for law enforcement to demonstrate that not enough real pizzas were sold, and so that the business must be partly fraudulent. However, this mechanism depends on the claim that many customers pay with cash, and this is becoming less and less sustainable as debit cards etc. are more widely used, even for small purchases.

Another suitable business is art, because the costs of the raw materials to create, say, a painting are small compared to the selling price, which could be a million times greater. The art market worldwide is

secretive, and anonymity of purchasers is commonplace. It is possible to create an art dealership and generate paintings that are apparently sold for large sums in cash to unidentified buyers. The sums paid by these fictitious buyers are made up from the laundered cash. This mechanism is more difficult to use than creating retail businesses, since it requires an art expert and an art creator who is good enough to create works with plausibly large prices (although, because "art is in the eye of the beholder", the property of being good enough includes substantial wiggle room).

Businesses where large amounts change hands can also be exploited, for example casinos, where wins that are provably legitimate can be bought at a discount price from winners desperate for quick money. However, casinos are amongst the most instrumented and analysed locations in the world, so any interaction within a casino risks leaving a record, visible both the casino analytics and potentially then to law enforcement. Despite this, casinos continue to play a substantial role in money laundering.

Banks in several Western countries have mechanisms that allow anonymous cash deposits, although into known accounts. In Australia, ATMS allow deposits of large amounts of cash, often into accounts set up by foreign tourists for plausible purposes. In Canada, cash deposit mechanisms are a holdover from the days when many businesses needed to deposit cash takings after banking hours. Amounts of the magnitude of around $25,000 can be deposited in this way, and then moved through the domestic financial system and between banks, so that the trail is difficult, perhaps impossible to follow.

Within a single national jurisdiction, there are fewer and fewer ways to convert cash to other kinds of mainstream assets without drawing attention. Moving money across borders, although it increases some kinds of risks, also has advantages because of the weaknesses of national government organisations at cooperation with other countries. Also many countries have little interest in money laundering, and so serve as havens for doing so.

International money laundering.

The main reasons for money laundering across national borders are that it provides both a natural break in the chain of ownership and discontinuities in jurisdiction. Although law enforcement organisations cooperate between countries, this cooperation is usually more difficult than within a single country, with different laws applying, different search and seizure rules, and different priorities. Tax departments also tend to be nationally focused.

It is also common for those who benefit from criminal activity to live in countries other than those where the crimes are committed. For example, the heads of drug production and smuggling cartels tend to live in Central and South America, while their profits are primarily made in the U.S. and Brazil. To access their profits, these must be moved from one country to another.

There are three qualitatively distinct mechanisms for moving money across borders, each with their own issues: objects of value can be physically moved; money can be moved through the global financial system; and value can be transferred virtually, that is without any actual movement of anything.

Moving objects of value.

The most obvious way to do this is to move cash physically. Travellers are supposed to declare amounts above a certain threshold (the $10,000 limit), but it is far from clear how likely someone carrying large amounts of currency is to be detected, either as an outgoing passenger (where checks are quite weak) or at Customs as an incoming passenger (which might be riskier, except that the countries where transnational criminals reside also tend to be those with weak border controls). For example, the U.S. estimates that at least $40 billion in physical currency is smuggled across the U.S.-Mexico border each year, while

programs aimed at finding and stopping it have interdicted less than $100 million. Currency can also be shipped as cargo and, again, the level of risk this carries is far from clear. There have been a non-trivial number of interdictions of currency in air shipments, and in vehicles across land borders. The reluctance of retailers to accept any but pristine U.S. dollar bills in South America suggests that owning bills that are visibly used attracts suspicion in those countries. This in turn suggests that authorities in those countries are aware of illicit US currency shipments that end up in circulation in South American countries. One of the problems with currency is that it is quite bulky for its value, and sometimes has a detectable smell (e.g. U.S. dollars).

The practice of smurfing, carrying currency just below the declarable amount across a border, is common and existing legal regimes make this difficult to suppress.

Another way to move value is to convert cash into small, portable, valuable items and transport these instead. The difficulty here is that the purchase of such items for cash is increasingly raising suspicion, as described above (although a number of small purchases over time could build up a reservoir of valuable items – for example, stored value cards can be purchased in modest quantities at a time, while accumulating large totals). The exception is art, for which large cash purchases are still the norm. Art has the added advantage that its declared value for border crossing need have little to do with its realisable value, and so it may not draw much attention from Customs. Thus while smuggling high-value diamonds carries some risk, smuggling art is almost totally without risk.

Bearer negotiable instruments also provide a way to move value (still with the risks associated with obtaining them). These are almost impossible to detect at borders, since they can be embodied in a single piece of paper. In some jurisdictions (e.g. Australia) there is no requirement to report a bearer negotiable instrument sent by mail.

Another way to move value is invoice fraud. A shipper in country A sends a legitimate product to country B but charges an exorbitant price for it. When the recipient pays the exorbitant price, a confederate in country A receives the difference between the actual price and the exorbitant price from the shipper so that value is transferred from country B to country A.

Moving money through the global financial system.

The global financial system exists to move money between countries, but such movements must be traceable by the financial institutions involved, and the records of these movements are increasingly accessible to governments. Thus a criminal moving money internationally must take steps to make the records of the movements seem innocuous. Banks are supposed to report transfers that they consider suspicious. The extent to which banks take this seriously, and their working definitions of ‘suspicious’ are far from clear, but many are looking for patterns of transfer that are *structured*, that is broken up into several sub-transfers, each designed to look innocuous. Another strategy used by criminals to further blur the existence of a large transfer is to send sub-transfers from different bank branches, using variant names and details of the sender, and using other techniques to disguise the similarity of the sub-transfers. Any one of the individual sub-transfers is designed not to seem suspicious at the particular branch; but it is not difficult for the bank to detect the overall structure, if it looks for it. There are limits to how much this can be done because the receiver needs to know that the correct total amount has been transferred, and in a timely way; too much blurring of sub-transfers creates opportunities for the sender to purloin some of the money. Banks are increasingly validating precise details of senders in their online transfer interfaces, making it harder to create artificial variations from one sub-transfer to another.

Banks continue to collude, at some level, with money laundering. There have been many recent fines imposed on well-known banks: most recently Danske Bank's branch in Estonia, a branch with only slightly more than a hundred staff, moved 200 billion euros over 8 years without any eyebrows being raised.

Moving value virtually.

There are a variety of alternative remittance systems (ARSs), of which the best known are the *hawalas*, that developed to facilitate transfers for people who do not have easy access to banks, or for whom the fees charged by mainstream financial institutions are prohibitive. Historically, the customers of these ARSs were guest workers in rich countries who send a portion of their wages to relatives back home.

When the flow from country A to country B is more or less in balance with the flow in the reverse direction, ARSs need move no money at all. Customers in country B receiving (notionally) money sent from country A are in fact paid with money deposited in country B intended for country A, and *vice versa*. Short-term imbalances are handled on a trust basis by the ARS bankers at both ends.

A problem arises when the flows between the two countries are not balanced, so that there is a net flow in one direction. The most common net flow is from rich countries to poorer ones and this is also the more probable direction for money laundering flows as well (although people smuggling, for example, may generate flows in the other direction). Net flows must eventually be realised as actual flows.

One way to handle the actual flow is to use conventional financial system transfers. A single financial system transfer is the result of the net of many small transfers collected and aggregated, so the overhead of a standard banking transfer is amortized. The effect of money laundering flows can be concealed in the larger flows arising from ordinary practice. Concealment is sometimes helped by the informal record keeping of many ARSs, although they are now registered in some jurisdictions, and so tracking mechanisms are beginning to be put in place.

The second way to handle the required balancing flows is to use cuckoo smurfing. This technique uses a legitimate transfer, in the direction opposite to that required to correct the imbalance, as cover. In other words, if ARS A wants to move $50,000 from to ARS B to correct an imbalance, they find a legitimate transfer from a customer of B to a customer of A of the right size, B takes the deposited funds from B's customer and keeps them, while A pays $50,000 to A's customer. Both customers are satisfied, A is $50,000 poorer while B is $50,000 richer, as required, and no money has actually moved through the global financial system. In fact, the only way to detect that this has happened is that the apparent transfer from B's customer to A's customer did not leave a trace, when it should have.

The same mechanism can be used directly for money laundering, as long as a matching countervailing innocent flow is available. The lack of trace of the money laundering transfer makes this approach especially attractive.

Cuckoo smurfing requires the existence of substantial innocent transfers in the opposite direction to the net flows between the two countries concerned (typically from poorer countries to richer ones) which may limit the applicability of this technique.

Many developed countries are on a trajectory to block most of these money laundering paths by more detailed regulation, and increased enforcement. However, Financial Intelligence Units (FIUs) – Austrac in Australia, Fintrac in Canada, Fincen in the U.S., and the Financial Intelligence Unit in the U.K. for example – struggle to find and/or block money laundering for several structural reasons.

First, the cornerstone of detection is the reporting, by banks and ASRs, of transactions that they consider to be suspicious or anomalous. While legislation lays out the conditions that should trigger reporting, there is, inevitably, some interpretation leeway; dealing with rich customers is how banks make their money; and so there is some incentive to under-report certain kinds of transactions. In other words, banks make a policy decision about the level of risk they will take, and this decision is not necessarily one that FIUs would agree with. In Zapata *et al.* v HSBC Holding Plc (2016), HSBC admitted criminal liability for laundering $881 million of the drug cartel proceeds, accepting large sums of money from individuals with no visible source of income. In several other successful terrorist financing prosecutions, well-known multinational banks transferred millions of dollars to terrorist organisations. The Commonwealth Bank of Australia was recently charged with failing to report more than 50,000 suspicious transactions over the $10,000 threshold, involving large deposits (100s of millions) paid in through ATMs and almost immediately transferred offshore. This suggests that, as well as developing regulations, FIUs need to be more aggressive in their approach to banks. Another aspect of the problem is that FIUs don't know about the transactions that they aren't told about, so it is difficult for them to assess the extent of under-reporting. Measuring compliance remains a challenge.

Second, money laundering has become a service, provided by specialists and marketed to criminals. A criminal group can outsource its money laundering needs to an organisation that develops its own intelligence, mechanisms, and experience in the use of techniques for laundering. More importantly, though, the use of such a wholesaler breaks the connection between the crime(s) that generated the money and the money itself – so that proving that intercepted money is actually proceeds of crime becomes much more difficult. When FIUs find transfers that are clearly suspicious, they may be unable to prosecute anyone because they cannot demonstrate that the money is not innocent. There may be a greater role for disruption as a strategy rather than prosecution, as the U.K already does.

One development which will change the face of money laundering is the development of cryptocurrencies such as Bitcoin. These make it possible to decouple the relationship between criminal and crime. For example, drugs are increasingly sold online via Dark Web market sites. Drugs are paid for with Bitcoin and shipped to the buyer through regular postal channels. These market sites operate like other online businesses, in some cases guaranteeing refunds if shipments are interdicted by Customs. But now criminals are paid in untraceable Bitcoins, and it is the buyers who have to convert traceable national currency into untraceable (and international) cryptocurrency. Bitcoin is already accepted by some real-estate brokers, some airlines and travel agencies, and sites such as eBay, so that criminals can spend their Bitcoin on their lifestyle directly. There are also arbitrage businesses that use Bitcoin to buy gift cards which are widely usable. The development of ransomware, for which the ransoms are also collected in cryptocurrency, shows how non-physical criminal 'services' can also be delivered without providing a path back to the criminals involved.

Another form of illicit money transfer that is not, strictly speaking, money laundering is the movement of money for evasion of tax. Many forms of tax evasion/avoidance seek to move money without revealing its ownership. Even when ownership is visible, international transfers can be used to reduce the tax payable. An individual in country A sends some money to country B using a mechanism that makes it non-taxable in country A (for example, a charitable donation). This money is then moved to country C and is then brought back to country A as incoming money that is again not subject to tax (for example, an international business loan). The money is now available to its original owner but has been sheltered from tax liability. This is difficult for financial authorities in any of the three countries to detect, since it seems innocuous until the loop is visibly closed.

One of the most hopeful developments in controlling money laundering is the development of Unexplained Wealth Orders (UWOs). These allow a government to ask an individual or business to show where the money it holds came from. This is a natural extension of the age-old police technique of looking from criminals who seem to be suddenly rich, or those who are living above their apparent means. UWOs have been used, although in a very limited way, in the UK to detect individuals moving illicit money from other countries as they settle in the UK. Popular targets are oligarchs from Russia and African dictators, both of whom find the UK a pleasant retirement place.

The benefit of UWOs is that they require no attention to where the money came from or how it arrived in the possession of the person of interest. The burden of proof has flipped from requiring law enforcement to demonstrate that the money is the proceeds of crime to the person of interest to demonstrate that the money has been gotten legitimately. Countermeasures to UWOs are difficult, because they rely on detecting spending; and if a criminal cannot spend his/her ill-gotten gains, what is the point? Of course, one workaround for criminals is to create apparently thriving businesses which account for the income, but it is hard to design a business generating large profits from small customer payments.

UWOs, of course, introduce legal problems because they impinge upon the presumption of innocence present in the common law of many countries. However, reverse onus already exists in several settings, and it may be possible to craft the law around UWOs to thread this needle. In the UK, UWOs are a civil mechanism and information gleaned in their use cannot be used for criminal prosecution. They result in confiscation of assets rather than jail terms – but this would be a strong deterrent for money laundering.

(Fear not, Dear Reader, that this document reveals anything to criminals that they don't already know. All of the content is already available from public sources.)