Data on bank transfers:

Complementing automatic exchange of information and detecting illicit financial flows in real time

Andres Knobel*

July 10, 2019

Summary

The lack of transparency in the international financial system facilitates illicit financial flows related to money laundering, corruption and tax abuse. Illegal and illicit activities have become increasingly sophisticated while countries struggle to detect them. To tackle this, authorities should apply advanced data analytics to the millions of daily financial transfers to discover suspicious transactions. The SWIFT messaging standard currently used by thousands of financial institutions represents a low-hanging fruit because it already centralises information on cross-border transfers which allows SWIFT to offer compliance products for banks and financial data to the US to fight terrorism. First, countries should collect and analyse all financial transaction data, either domestic or those coming in and out of their territories (including those that don't use SWIFT messaging). Secondly, an international organisation should have access to anonymised SWIFT data in order to take the wider picture into account and detect red flags involving multiple jurisdictions that can then be reported to the jurisdictions involved. Thirdly, while SWIFT already publishes some statistical data on the number of SWIFT messages, their distribution by market and their distribution by region, it should also publish anonymised and aggregated data on all international transfers at a country level, so that civil society and investigative journalists have access to basic data and can hold authorities to account.

* This proposal follows from discussions between Jeffrey Sachs, Jim Henry and Alex Cobham (Ethics in Action, Alpbach, August 2018). This paper received invaluable contributions from Howard Cooper, Joshua Kirschenbaum, Andres Arauz as well as from Lakshmi Kumar, Sakshi Rai and Matti Kohonen, all in their personal capacity. However, the views expressed are solely those of the author and do not necessarily represent those of the contributors.

Background

Financial secrecy is the common denominator that enables illicit financial flows related to tax evasion, tax avoidance, corruption, money laundering and the financing of terrorism, among others. These illicit activities flourish whenever the identity of criminals, their assets and their income manage to remain secret. The Tax Justice Network and other civil society organisations, eg the Financial Transparency Coalition, have been calling for more transparency for years as a way to tackle illicit financial flows. The ABCs of tax transparency, a simple proposal for beginning to dismantle financial secrecy, call on countries to implement the following:

Automatic exchange of financial account information with all countries and to publish statistics about the information being exchanged.

Beneficial ownership registries – available to the public, online, for free and in an open data format – identifying the individuals who ultimately own, control and benefit from legal vehicles (eg companies, partnerships, trusts and foundations).

Country-by-country reporting to be publicly available online, where multinational entities describe the activities, assets, employees, income and taxes paid in each jurisdiction where they operate.

Wealth data

Information about wealth is indispensable to identify tax evasion, corruption and money laundering. For example, finding out about someone's real wealth could indicate not only whether they have paid all applicable income and wealth taxes, but also if they can justify the legal origin of that wealth ("how do you have so much money in the bank and own so many mansions if you only declared a public officer's salary?"). The Tax Justice Network is currently working with the Independent Commission for the Reform of International Corporate Taxation (ICRICT) to develop a framework for a Global Asset Registry based on the proposal by Thomas Piketty and Gabriel Zucman.

Of all the possible forms of wealth (such as cash, art, gold, real estate, investments in securities, etc.), countries have only really made progress on beneficial ownership transparency at a global level in relation to financial accounts, (for example, banking information), in addition to some incipient local measures[1] for real estate. There is little or no beneficial ownership transparency with respect to wealth held in other forms.

[1] For example, the UK and the US have made some progress in relation to identifying the beneficial owners of entities owning or acquiring real estate in certain areas. See for example: https://www.theguardian.com/business/2018/jul/23/offshore-owners-of-british-property-to-be-forced-to-reveal-names and http://www.fcpablog.com/blog/2018/11/16/fincen-expands-beneficial-owner-reporting-for-cash-real-esta.html

Automatic exchange of information on bank account balance and income

Global access to banking information has experienced significant progress with the implementation of automatic exchange of information (AEOI) under the OECD's Common Reporting Standard (CRS). Around 100 jurisdictions have started to exchange granular banking information with each other, reporting the identity of each account holder and in many circumstances the beneficial owners of the account also[2].

Even though automatic exchange of banking information may in principle be used for tax purposes only, some countries[3] have committed to using this information to tackle corruption and money laundering as well, as suggested by the Tax Justice Network and the Financial Transparency Coalition in the past[4].

However, automatic exchange of information under the CRS only includes a snapshot of information on the account balance on a particular day (generally, December 31st,) as well as the total income generated (such as interest or dividends, depending on the type of account) received in a year. A snapshot of someone's bank account balance would only reveal corruption or money laundering if the account holder could not justify why they have so much money in the bank compared to their declared income. However, a sophisticated money launderer would hardly be so careless, given that exactly when the snapshot will be taken is public information—usually December 31st of every year. They can easily escape notice simply by taking the money out on December 30th and returning it on January 1st.

To tackle these simple avoidance strategies, it is necessary to provide not just a snapshot, but the whole "movie" – that is, all bank transfers and all fluctuations in account balances and income. Information on bank transfers can also play a vital role in complementing the automatic exchange of information: it can be used to detect money laundering schemes on a grand scale and even in real time.

Banks and money laundering

As confirmed by recent scandals like the Panama Papers and the Russian and Azerbaijani Laundromats, as well as by evaluations conducted by international organisations such as the OECD's Global Forum and the Financial Action Task Force,

[2] When the bank account holder is an entity (instead of an individual) and this entity is engaged in mostly passive income (eg income from interest, dividends, royalties), banking information to be exchanged includes the identity of the "passive" entity and of its beneficial owners. By contrast, when the account holder is an entity considered "active" (eg because it provides goods or services), only the entity is identified, but not its beneficial owners. For these cases, public registries of beneficial owners available in some countries may complement the missing data (to find out who the beneficial owners of the "active" entities are).

[3] See the OECD's Punta del Este Declaration: https://www.oecd.org/tax/transparency/Latin-American-Ministerial-Declaration.pdf

[4] https://financialtransparency.org/wp-content/uploads/2016/05/Letter-to-OECD.pdf

illicit financial flows are thriving while compliance with international transparency standards and with anti-money laundering recommendations remains low[5]. Meagre rates of effective compliance are evident[6] in the legal frameworks of many countries (both developed and developing); the activities of financial institutions, lawyers and corporate service providers; and the supervision of these financial institutions and professionals by government authorities.

Global Financial Integrity[7] has identified some of the worst offending banks sanctioned for money laundering in 2018 including UBS, Rabobank, the Commonwealth Bank of Australia and US Bancorp. Others include Danske Bank[8] and Deutsche Bank[9].

On top of this, financial crimes are becoming increasingly sophisticated, with artificial intelligence now being deployed to design money laundering transactions that are undetected by current systems. So beneficial ownership transparency and full compliance with current anti-money laundering recommendations alone cannot solve this issue. Even for a bank properly implementing "know-your-customer" policies, it may be impossible to detect an international money laundering scheme that involves many accounts in many banks in many countries using current transparency tools. It is essential for transparency improvements to keep pace with constantly evolving technology.

Data on bank transfers to detect money laundering.

To identify these international money laundering schemes and complement national anti-money laundering measures, it is necessary to look at the big picture and apply advanced analytics, as exemplified by Howard Cooper at the 2018 International Anti-Corruption Conference[10]. By centralizing information on all international banking transactions and applying the necessary analyses, including big data, it would be possible to identify unusual situations, like a high number of transactions shuffled across different bank accounts that belong to the same beneficial owner and make no commercial sense.

National experiences

Several successful national experiences and proposals demonstrate how to use financial information to detect illicit financial flows and can inform an improved path forward in combatting financial secrecy.

[5] http://www.fatf-gafi.org/media/fatf/documents/4th-Round-Ratings.pdf
[6] https://www.fatf-gafi.org/media/fatf/documents/4th-Round-Ratings.pdf
[7] https://www.gfintegrity.org/taking-stock-of-2018-part-1/
[8] https://www.ft.com/content/6ae5f7f6-f324-11e8-ae55-df4bf40f9d0d
[9] https://www.bbc.com/news/business-46382722
[10] https://iaccseries.org/blog/using-data-to-counter-corruption-and-money-laundering/

a) Norway

Norway established the Central Currency Register that collects information on all payments to and from another country, the use of Norwegian cards abroad, the use of foreign cards in Norway, and the exchange of bank notes above 5,000 NOK[11] (ca. USD 600). A report[12] by the World Customs Organization describes successful stories of the currency register: detecting social security fraud (beneficiaries have to live in Norway, so if money is being withdrawn in Poland or Nigeria, this becomes suspicious); identifying trade mis-invoicing where the declared import or export value does not match the payment for those goods registered in the currency register; and the potential to prevent terrorism (out of 41 money transactions involving the acquisition of chemicals from a foreign country and reported to the police as suspicious, one referred to the terrorist who killed 76 people in Oslo in 2011).

b) The United States

Joshua Kirschenbaum, Senior Fellow at the Alliance for Securing Democracy, has urged the United States to create a centralised database of all international funds transfers that transit the US as a way to detect (for example, Russian) illicit financial flows affecting the country. He proposes that "large New York banks that clear dollars for international payments would report the data on a near real-time basis. The reporting streams could then be combined, providing a complete view of U.S. dollar transactional activity. The idea has been studied by the Treasury Department but never finalized, although Canada and Australia collect this type of information. While international funds transfer records are available on an ad hoc basis, only a centralised database would drive the type of powerful analysis that is necessary. With a central repository in place, the U.S. government can ask questions like, 'How much money flows between banks in Cyprus, Latvia, and Russia? Has there been a shift in the pattern in past months?' If a small bank suddenly and rapidly increases its level of dollar clearing out of proportion to the business profile of its customers, the shift will set off an immediate red flag. And the government will have more granular information about how much money moves from Russian banks to U.S. banks, or vice versa.'"[13]

c) Brazil

Brazil for many years levied a financial transaction tax (CPMF, literally translated as a provisional contribution on financial transactions), levied on each bank transaction that took place in Brazil. In doing so, it not only raised revenue (approximately $20 billion per year in its last year of operation in 2007), it also created a database of all financial transactions in Brazil that authorities could use to track corruption, tax

[11] https://www.dnb.no/en/business/markets/foreign-exchange/currency_register.html

[12] http://www.wcoomd.org/-/media/wco/public/global/pdf/media/newsroom/reports/2018/wco-study-report-on-iffs_tm.pdf?la=en

[13] https://securingdemocracy.gmfus.org/tracking-illicit-russian-financial-flows/

abuse, tax evasion and money laundering. One expert commented in an interview that:

"Many people hate this tax is because [sic] it simply cannot be evaded unless you keep your money under a mattress. Banks are designated agents of the Treasury for tax collection and come under intense scrutiny, so they will deduct that 0.38% every Friday. The second (unspoken) reason many people hate this tax is because the year-end CPMF numbers are made available to the Revenue Service (SRF) to check income tax returns. If you declare R$10.000 of income, but ran R$1.000.000 through your account, that raises a red flag and you may get audited. If there's no more CPMF, there's no more reality check. Hooray! If you combine these two reasons, you arrive at the following conclusion: only people who work on an 'off books' basis, in the 'parallel' economy, truly hate the CPMF."[14]

The use of a national tax as a basis for creating a national database of all financial transactions is one method for creating the necessary information that is then used by different relevant authorities. It could have also been released in an anonymised form to researchers as proposed above, but that was not done, and the data may now already be lost. It is not known how many cases of money laundering, tax evasion and abuse were uncovered based on this data.

d) Colombia

Colombia has in place a foreign financial transaction tax called GMF that applies to any type of financial transaction resulting in Colombian funds being transferred outside of Colombia. The tax is a flat rate of four tenths of one percent (0.4%) (colloquially referred to as 4 per 1,000)[15]. Half the total tax paid is deductible for income tax purposes, regardless of whether or not the transactions have a causal nexus with the income producing activity of the taxpayer. The financial transactions tax, formally known as *Gravamen a los Movimientos Financieros* (GMF), is a permanent tax on financial transactions, the collection of which is the responsibility of regulated financial institutions and of the Colombian Central Bank (*Banco de la República*). The taxable event is the carrying out of financial transactions that involve the disposal of resources deposited in checking or savings accounts with a bank based in Colombia, as well as in deposit accounts with *Banco de la República*, and the issuance of cashier's cheques. In other words, GMF applies to any type of financial transaction resulting in Colombian funds being transferred outside of the country.

According to the Colombian tax and customs authority, the GMF has served as a way to reduce tax evasion in Colombia[16]:

[14] https://www.taxjustice.net/2015/09/10/will-brazils-cpmf-financial-transactions-tax-live-another-day/
[15] http://taxsummaries.pwc.com/ID/Colombia-Individual-Other-taxes
[16] https://www.dian.gov.co/dian/cifras/Cuadernos%20de%20Trabajo/Generalidades%20del%20gravamen%20a%20los%20movimientos%20financieros%20(GMF)%20en%20Colombia..pdf

"Among the advantages it is also recognized that the tax has served the State as an element of control to reduce evasion. Despite the preference for cash management that the GMF can generate, the need that the different economic agents have when they carry out multiple commercial transactions, to use the financial sector, reduces the possibilities of hiding these transactions for the determination of other taxes such as income and VAT. "

An existing source for all countries: SWIFT

For all countries, especially those that are not major financial centres, there may be a much simpler solution. SWIFT is mostly known for providing a network that enables financial institutions worldwide to send and receive information about financial transactions in a secure, standardized and reliable environment. More than 11.000 institutions in more than 200 countries and territories use SWIFT. In 2017 alone, there were 7.1 billion messages[17] about financial transactions. Using the vast amount of data on international transactions that passes through its system, SWIFT is now offering compliance analytics to banks that assess the institution's financial crime risks across its operations and network. According to SWIFT's website[18], compliance analytics will allow banks to "identify anomalies in behaviour, unusual patterns or trends in traffic flows, hidden relationships, and significant levels of activity in high-risk areas… to develop risk models, set alerts to highlight specific areas of risk within their business, and benchmark themselves against their industry peers". If individual banks can obtain so much value out of their own SWIFT data for compliance purposes, a country should be able to do so much more with access to the same data, especially since their data would include all local financial institutions rather than just one.

Therefore, similar compliance analytics, but at a larger scale (not just for one bank, but for a number of countries) would be a key tool for tackling international money laundering schemes. One possibility would be for SWIFT to run big data analyses based on a set of criteria developed by an international group of experts (eg Egmont Group) to **identify and communicate** any red-flag transactions to the relevant financial intelligence units. Alternatively, SWIFT could share the bulk data with a designated international authority or with financial intelligence units to use for their own analyses and investigations. SWIFT already offers data on cross-border flows to Central Banks to monitor monetary policies, so sharing similar financial transaction data with financial intelligence units should not present any obstacles.[19]

Some countries are already using SWIFT data for prevention of illicit financial flows. For example, after the terrorist attacks of September 11th, 2001, the US initiated the

[17] https://www.swift.com/about-us/highlights-2017

[18] https://www.swift.com/news-events/press-releases/swift-launches-compliance-analytics-service-to-help-banks-manage-financial-crime-risk

[19] https://www.swift.com/our-solutions/compliance-and-shared-services/business-intelligence/swift-scope/for-central-banks

Terrorist Finance Tracking Program (TFTP) to obtain information and counter the financing of terrorism. Based on this program, SWIFT must provide certain financial transaction records (in the form of SWIFT messages) required by the US Treasury.[20] SWIFT data appears to be so valuable, that the US Treasury reported "SWIFT information greatly enhances our ability to map out terrorist networks, often filling in missing links in an investigative chain… By following the money, the TFTP has allowed the U.S. and our allies to identify and locate operatives and their financiers, chart terrorist networks, and help keep money out of their hands."[21] The European Union should do the same.

Ecuador is taking a similar approach but based on financial information that local banks report to the banking regulator. On one occasion, aggregated SWIFT information was made public after a congressman requested it. This allowed researcher Andres Arauz[22] to estimate and identify the destinations of capital flight fleeing Ecuador.

SWIFT data could also be used to detect international trade mispricing and triangulations, similar to Norway's Central Currency Register, given that the declared price and destination or origin of an export or import of goods should be matched to a specific payment. In addition, information could include whether the bank account holder refers to an individual, a company or a trust, in order to detect patterns based on the type of legal vehicle involved in the financial transaction.

SWIFT statistics for all

In addition to allowing authorities to detect illicit financial flows, SWIFT should also publish aggregate information about international banking transfers based on the country of residence of the legal and beneficial owner. In this way, authorities from countries unable to obtain SWIFT bulk data (due to legal reasons or confidentiality concerns), civil society organisations, and journalists would all be able to access the big picture of total transactions carried out by a country's residents as well as all transactions leaving and entering the county. This would allow researchers to identify flows of transfers that could be related to capital flight (eg if the money leaving a developing country to find shelter in a tax haven is greater than the money entering a developing country) or other types of illicit financial flows (eg if money from highly corrupt countries is entering or if most of the money entering a country comes from a small tax haven with a GDP much smaller than the flow of transactions). Statistics should also include the type of account holder (individual, company, partnership or trust) to detect patterns based on the type of legal vehicle involved in the financial transaction.

[20] https://www.swift.com/about-us/legal/compliance/tftp

[21] https://www.treasury.gov/resource-center/terrorist-illicit-finance/Terrorist-Finance-Tracking/Documents/TFTP%20Fact%20Sheet%20revised%20-%20(2-15-11)%20(2).pdf

[22] Presentation by Andres Arauz at the Tax Justice Network annual conference held in Lima, on June 14th, 2018 available here: https://www.youtube.com/watch?v=73qTILjTNAQ

While countries' statistics on foreign direct investment often detail country of origin, SWIFT data would make it possible to determine whether the investment truly originated in the presumed country of origin or whether the investment was merely rerouted through the country. Related to this, SWIFT is already offering a service for banks to assess the routing of flows to identify redundant intermediaries that could be eliminated to reduce costs and improve efficiency.[23] Based on this, SWIFT could allow investigators to determine whether an investment from the British Virgin Islands actually came from the tax haven or whether it originated in a sanctioned country and was rerouted through the tax haven.

The proposed publication of aggregate numbers on SWIFT financial flows should not be considered extraordinary. SWIFT already publishes monthly statistics[24] on the quantity of SWIFT messages, their distribution by market (eg payments, securities, trade, etc), and their distribution by region (Europe, Middle East and North Africa, Americas, and Asia Pacific). In addition, the Bank of International Settlements publishes a country-level breakdown of deposits held in each country's financial institutions, and also basic data on SWIFT message flows sent and received by each country[25]. Countries[26] such as the US and Switzerland publish total liabilities by country of origin. Australia will publish statistics based on the OECD's Common Reporting Standard for automatic exchange of information. SWIFT statistics on financial flows would merely complement the public data about financial stocks that is becoming increasingly available.

RECOMMENDATIONS

Based on the explanations above, countries should sign an international convention to ensure that comprehensive data on financial transfers is collected and that advanced analytics are carried out at national and international levels to detect money laundering, and to complement automatic exchange of banking information.

1. Comprehensive data collection for further advanced analytics

a) All financial transactions must use SWIFT or collect consistent information

All countries should require every bank to apply SWIFT messaging to any domestic or foreign financial transfer (or to collect equivalent information), including all banks conducting international transactions within the same banking group. Data to be collected and reported by each bank should refer to the absolute value of each outward and inward transfer, regardless of whether values will be netted in practice.

[23] https://www.swift.com/resource/cross-border-payments-swift-data-and-insights-de-payment-flows
[24] https://www.swift.com/about-us/swift-fin-traffic-figures/monthly-figures?tl=en#topic-tabs-menu
[25] http://stats.bis.org/statx/srs/table/PS6
[26] See more details and sources here: https://www.taxjustice.net/2018/07/11/its-time-for-countries-to-start-publishing-the-data-theyre-collecting-under-oecds-common-reporting-standard/

In addition, and possibly as a second step, all international transfers taking place outside of the banking system (eg Western Union, Paypal, WeTransfer, etc) should either apply SWIFT or provide all relevant information to the central authority in charge of analytics (eg SWIFT or an international organisation to be designated, see below).

A later stage would require information on crypto-currencies to also be centralised for advanced analytics.

b) SWIFT data should include information on the ultimate beneficial owner

SWIFT messages have increased their details (eg from format "MT 202" to "MT 202 COV") to include more data (eg originator and recipient information) which allows intermediary banks to run anti-money laundering checks. The Financial Action Task Force on Anti-Money Laundering (FATF) Recommendation 16 requires that payment messages include complete remitter and beneficiary information[27,28]. However, even if banks were to fully comply with FATF Recommendation 16 and provide required information in SWIFT messages, this still refers only to legal ownership information, which is only of limited use[29]. A criminal could create many entities and use each of them to open different bank accounts. In this case, bank transfers among all the different entities created by one individual would look like isolated transactions. The only way to realise that they are all related to the same person would be for SWIFT messages to include not only the account holder information (eg the company holding the bank account), but also the "beneficial owner" of the account holder (the individual ultimately controlling or owning that company).

Based on the Financial Action Task Force Anti-money laundering recommendations, banks are already required to identify the beneficial owners of each account held by an entity (banks also have to identify the beneficial owners pursuant to the Common Reporting Standard for automatic exchange of information). This means that beneficial ownership information is already available at the banks. The only needed change would be for SWIFT messages to add a field that includes the identity of all beneficial owners of both the originating and recipient account holders.

This way, all the advanced analytics described above could be done at the beneficial ownership level to detect even more sophisticated cases of money laundering.

c) Validation of data populating SWIFT messages

At the very least, the SWIFT system should only accept messages that have all required fields and otherwise reject sending the message. For example, JPMorgan Hong Kong was fined for handling "wire transfers on the SWIFT messaging system

[27] https://www.swift.com/sites/default/files/resources/swift-compliance-casestudy-paymentsdataquality.pdf
[28] https://www.wolfsberg-principles.com/sites/default/files/wb/pdfs/wolfsberg-standards/1.%20Wolfsberg-Payment-Transparency-Standards-October-2017.pdf
[29] For this reason, many civil society organisations, including the Tax Justice Network, have been asking for international standards to be upgraded to require more transparency, eg public registries of beneficial ownership.

without including the names of the originators."[30] Secondly, SWIFT should require banks to establish a validation system that only allows matching information to be populated in SWIFT messages (eg the account number included in the SWIFT message must refer to an existing active account of a bank) or otherwise be rejected. Information on the account holder and beneficial owners should be automatically populated (rather than manually) based on the information held by each bank's records.

2. Data reporting and analysis at the national level

Each country (eg the Central Bank or the financial intelligence unit or financial supervisor) should require every local bank, regardless if located in a special economic zone or not, to provide all relevant local and cross-border transaction data (with all details included in SWIFT messages) to a central location for analysis. This would help reveal capital flight, trade mis-invoicing, or triangulations (if declared imports and exports don't match the payments). However, complex money laundering schemes involving multiple jurisdictions may still go undetected.

Major financial centres like the US and the European Union should require reporting of all national transactions and also of all international transactions carried out in local currency (eg USD or Euros cleared by local banks) for analysis.

3. Data reporting and analysis at the international level

To understand the "big picture" (cross-border transactions involving multiple jurisdictions that cannot be seen by any individual country alone), the international standard (codified, for example, in an international convention) should require SWIFT to give a designated international authority access to its cross-border transactional data in anonymised form[31]. This international authority could be for example integrated by the Egmont Group, who would be able to run advanced analytics on SWIFT data to find patterns and red-flag potential cases of money laundering. Another option would be for SWIFT to run the advanced analytics themselves, based on pre-set criteria and indicators established by a committee of anti-money laundering experts.

In the first option, the designated authority in charge of analysing SWIFT data, in addition to complying with the highest confidentiality and data security standards, would only have access to anonymised SWIFT transactional data (so no entity or

[30] https://www.bloomberg.com/news/articles/2018-12-28/hong-kong-watchdog-fines-jpmorgan-over-money-laundering-controls

[31] Based on the second point, requiring each country to collect information on all bank transactions reported by local banks, countries could share this country-wide information with each other, similar to automatic exchange of information based on the OECD's Common Reporting Standard (where Germany shares with France information on French account holders with accounts in German banks, and vice-versa). However, given that SWIFT already has centralised all the information (opposite to information on bank deposits which is not centralised by one authority), it is much easier to give access to SWIFT data than to set up a new mechanism to exchange bank transfer data.

individual would be identifiable, only red-flagged transactions involving entity X or individual Y).

While the identity of the bank, the account holder and the beneficial owner would remain anonymous, the database should allow all transactions corresponding to each bank, to each account holder and to each beneficial owner to be connected so that they do not appear as isolated and unrelated transactions. For example, anonymised data could show that account holder 1452 in bank 003 in Germany sent $1000 to account holder 152 in bank 34 in France; and $500 to account holder 178 in bank 78 in Belgium (if transactions of each bank and each account holder were not connected, no one would know that both transactions correspond to the same account holder, which may be extremely relevant to detect "atomized" money laundering schemes engaging in several small-value transactions).

The designated authority (or SWIFT, if they ran the analytics themselves) would share the anonymised (red-flagged) transactions with the relevant authority (eg the financial intelligence unit) of those countries involved in the suspicious scheme. In addition, these countries would be able to request SWIFT to hand in the identity of the local banks and local account holders involved in the red-flagged transaction, as long as the country complies with all confidentiality standards and appropriate use of information. The confidentiality and appropriate use of standards to access the identity from SWIFT could be based on the confidentiality provisions that countries are already required to meet in order to receive automatic exchange of information about bank accounts, pursuant to the OECD's Common Reporting Standard. After all, countries are already receiving the name, date of birth and tax identification number of each account holder holding a foreign bank account. The only difference in this case is that the data would refer to a bank transfer rather than a bank account balance.

4. Publication of SWIFT statistics (aggregate data)

Given that the access, analysis, and red-flags mentioned above will be confidential, SWIFT should annually publish the anonymised transactional data mentioned above, but on an aggregate level. For example, "In 2020, Bank 1 in Germany (or all banks in Germany) transferred $100 billion to banks in France, $50 million to banks in Spain; and received $100 million from banks in the US". This would allow civil society organisations, researchers, and journalists (as well as countries unable to receive SWIFT data for confidentiality shortcomings) to perform basic analyses of cross-border transactions. Additionally, reported statistics should allow observers to view financial transactions depending on the type of account holder (eg individual, company or trust) in order to detect patterns based on the type of legal vehicle involved in the financial transaction.

PROPOSAL FACTSHEET

1. Financial transaction data should include beneficial ownership data and be validated: countries should require that records of all financial transactions in their territory include beneficial ownership information on the sender and recipient of the financial transaction. Beneficial owners of transactions are already known because financial institutions are already required to identify the beneficial owners of their accounts to comply with know-your-customer regulations. Information should be validated (all fields should be completed before a transfer may take place, and information on account number, legal and beneficial owners should automatically be populated based on a bank's own records to avoid users manually filling data inconsistent with a bank's own records.

2. Centralisation of national financial transaction information: relevant information (including beneficial ownership data) should be available on all national financial transactions whether or not they are already covered by SWIFT or if carried out by banks, fintech companies or apps, or crypto-currencies. All of this relevant data on national financial transactions should be centralised by national authorities for analysis and detection of illicit financial flows (eg money laundering, financing of terrorism). Many countries already require banks to report banking data to authorities on a regular basis.

3. Centralisation of international financial transaction information: financial transactions involving all countries should be centralised by an international authority (eg related to the Egmont Group) to make it possible to see the "big picture" and identify complex money laundering schemes and other illicit financial flows involving many different jurisdictions. Financial transaction information could be anonymised for data protection purposes. The international authority (or SWIFT itself) should run advanced analytics on this centralised international financial transaction data based on preset criteria established by a committee of anti-money laundering experts. The international authority (or SWIFT) would then report any red-flagged transactions to the authorities of the countries involved, so that they may request the identity of the banks and individuals involved (as long as they comply with confidentiality provisions).

4. Publication of statistics: anonymised data on financial transactions should be aggregated and published for civil society organisations and journalists to have access to basic financial transaction information and to hold authorities to account.

* SWIFT: a long hanging fruit

SWIFT represents a low-hanging fruit to run a first pilot of this proposal. The advantage of this approach is that SWIFT already centralises information on international financial transactions from thousands of banks in most countries, and it already uses this information to provide compliance and other services to banks and national authorities. The disadvantage is that SWIFT does not collect information on the beneficial ownership level for the sender or the recipient of bank

transfers, and that certain financial transaction platforms do not use SWIFT messages (eg Paypal, Western Union or cryptocurrencies). Nevertheless, given that banks and the US government have been using SWIFT services and data for compliance and the fight against terrorism respectively, SWIFT data clearly has value that should be exploited by authorities from all countries worldwide.

To address SWIFT's disadvantages, countries should require SWIFT to incorporate beneficial ownership into its messaging system, and should require all international and national financial transactions (eg Paypal, Western Union, Bitcoins) to apply SWIFT or to report all relevant data to national authorities (and to the international organisation involved in the global advanced analytics).

FAQ

a. Could SWIFT incorporate beneficial ownership information? SWIFT messaging formats have been upgraded in the past, for example by increasing their details (eg from format "MT 202" to "MT 202 COV") to include more data (eg originator and recipient data) to allow intermediary banks to run anti-money laundering checks. They should upgrade again to include beneficial ownership data, which financial institutions are already required to obtain as part of their know-your-customer regulations.

b. "If authorities start using SWIFT data for anti-money laundering and counter-terrorism purposes, criminals will simply avoid using financial institutions that use SWIFT, so SWIFT data will become useless to prevent crimes". Ideally, all financial transactions (including cryptocurrencies) would be immediately collected and centralised for analysis. Realistically, however, that will take time. Most new transparency initiatives start with a limited scope (eg automatic exchange of banking information, country-by-country reporting by multinationals). While loopholes may indeed be exploited to circumvent the new transparency measures, the increased transparency does have value and also sends a message to the industry (and criminals) indicating that more transparency is to come, creating a deterrent effect. In the case of SWIFT data, the New York Times revealed that the use of SWIFT data by the US government started in 2006[32]. Nevertheless, it appears that SWIFT data is still relevant because thousands of banks and the US government continue to use SWIFT data even today for their compliance and anti-terrorism goals as described above.

c. "Sharing financial transaction data or publishing statistics would breach data privacy laws". More than 100 countries are already sharing banking information with each other, pursuant to international treaties that implement the OECD's Common Reporting Standard, sharing data on account balances, account holder and beneficial owner names, dates of birth and tax identification numbers. If exchanging information on banking account balance is legal, it would be hard to explain why information on bank transfers would breach any confidentiality or data

[32] https://www.nytimes.com/2006/06/23/washington/23intel.html

privacy, assuming an international treaty provides a legal framework for its exchange. Besides, countries are already allowed to request bank transfer data from foreign authorities based on double tax agreements or tax information exchange agreements. As for sharing information with the international organisation for centralisation and analysis, this data may be anonymised so that no confidentiality is breached. In regard to publishing statistics, SWIFT, the Bank of International Settlements, and many countries' Central Banks already publish financial statistics by country of origin. In the case of this proposal, information would not only be anonymised, but it would also be aggregated, indicating only the totals by the account holder's country of residence. In other words, publishing information, for example, "all German banks transferred a total of 100 million Euros to banks in France in 2018" would hardly breach any German confidentiality laws.