

May 25, 2016

Mr. Je-Yoon Shin
President
The Financial Action Taskforce (FATF-GAFI)
2 Rue André Pascal
75775 Paris
France



Dear Mr. Shin:

Re: Facilitating effective sharing of AML/CFT information

The Institute of International Finance (the "IIF" or the "Institute") appreciates the opportunity to provide input to the Financial Action Taskforce (the "FATF") as it works to address many of the key issues facing the global financial community today. As a permanent member of the FATF Private Sector Consultative Forum ("PSCF"), the IIF has long supported the goals of the FATF in promoting effective implementation of measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system.

The Institute has been working closely with its members and the public sector to evaluate areas where the efficient work of the system to fight financial crime may be impeded or where certain issues could lead to unintended consequences. This has produced discussion and recommendations specifically around de-risking in correspondent banking¹, and has also initiated discourse on the wider components of a well-functioning anti-money laundering and counter-terrorist financing ("AML" and "CFT") infrastructure. One of the cornerstones of this framework is effective information sharing, both within the private sector and between the private and public sectors.

We are pleased this issue has been recognized by the FATF and that it formed an integral part of the most recent PSCF in Vienna, Austria in April 2016. Building on the exchange of views at that forum, the IIF is grateful to present our additional feedback for consideration by the FATF at your upcoming June 2016 plenary meeting in order to assist in your efforts in determining next steps to tackle the information sharing barriers that have been identified in the enterprise-wide context, among financial institutions not part of the same financial group, and between governments and the private sector. The specific challenges to effective sharing of AML/CFT information - such as the impact of inconsistent legal frameworks for data protection and privacy across different jurisdictions - are essential to be overcome in order to better ensure stability and security in global finance. Our comments are given on the basis of a profound commitment by the international banking industry to maintain and enhance the integrity of the global financial system and to help the appropriate authorities stop abuses.

¹ For further information on this issue, please see the IIF/BAFT Letter to the CPML dated December 7, 2015: <https://www.iif.com/publication/regulatory-comment-letter/iifbaft-joint-response-cpml-correspondent-banking>

Specifically, we believe there are two areas where further consideration and action by the FATF in June would be beneficial:

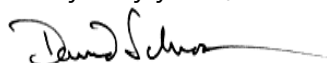
- The agreement by the FATF to update the FATF Recommendations to enable more effective information sharing in the enterprise-wide context, among financial institutions not part of the same financial group, and between governments and the private sector (please see the case study below which gives specific examples of obstacles to information sharing which are not explicitly covered in the FATF Recommendations);
- The agreement by the FATF to analyze among its members the jurisdictional legal impediments to information sharing, based on an upcoming IIF industry survey concerning these issues.

To assist in these efforts, the IIF submits herein our preliminary proposals on updates to the FATF Recommendations to better facilitate information sharing. We also set out a detailed example outlining information sharing barriers across jurisdictions in order to illuminate the scope of the problems facing the industry, national governments, and international bodies. In particular, we are committed to assist the FATF in the examination of jurisdictional legal impediments highlighted in the illustration by conducting an industry survey of our member institutions to provide an analysis of the scope of the issues needing to be addressed. As a first step however, we respectfully encourage the FATF to agree the above action items in June as an important way forward in the work to protect the integrity and security of global finance.

We emphasize that this is a preliminary submission by the industry and we look forward to a more detailed exchange with the FATF, alongside the Basel Committee, the Financial Stability Board (“FSB”) and the Committee on Payments and Market Infrastructures (“CPMI”), on these matters as discussions develop in coming months. As part of this, we also encourage a holistic and coordinated review of improving information sharing to tackle financial crime in all areas and by all relevant stakeholders. We are encouraged by the recent G-7 statement calling for the enhancement of information exchange and cooperation for CFT purposes.² However, such action undertaken by the FATF and others to improve this issue should be broadly applicable beyond CFT in order to help standardize the tools to combat all bad actors in the system so effective results are not siloed.

Thank you very much for your consideration of our feedback and proposals. Should you have any questions, please do not hesitate to contact me or Matthew Ekberg (mekberg@iif.com).

Very truly yours,



David Schraa
Regulatory Counsel

² G7 Action Plan on Combatting the Financing of Terrorism; May 21, 2016:
http://www.g7sendai2016.mof.go.jp/summary/pdf/g7_action_plan_on_cft_en.pdf

1. IIF preliminary proposals regarding information sharing amendments to the FATF Recommendations

The FATF Recommendations³ on a comprehensive and consistent framework of measures which countries should implement in order to combat money laundering and terrorist financing are critical to the safety and security of the international banking system. The IIF believes, however, that the Recommendations would benefit from clearer guidance to enable more effective information sharing in the enterprise-wide context, among financial institutions not part of the same financial group, and between governments and the private sector. As such, the IIF proposes preliminary consideration of the following amendments to the Recommendations, subject to further dialogue with the industry:

- Countries should ensure that financial institution secrecy laws, data protection and data privacy laws, outsourcing laws and tipping-off provisions do not inhibit the exchange of information relating to customers, accounts or transactions (including suspicious activity reports (“SARs”) and associated underlying information)⁴ between entities in the same corporate group for the purpose of financial crime risk management, including when such exchange takes place between entities in that same corporate group but in different jurisdictions.
- Countries should ensure that financial institution secrecy laws, data protection and data privacy laws, outsourcing laws and tipping-off provisions do not inhibit the exchange of information relating to customers, accounts or transactions (including SARs and associated underlying information) between entities in different corporate groups for the limited purpose of financial crime risk management (such scope to be determined).
- Countries should ensure that adequate legal protections are in place to facilitate the sharing of information in the circumstances described above under appropriate “safe harbor”.
- Countries should ensure that laws requiring a financial institution to file a report to either a local or foreign regulatory body or law enforcement agency under the above circumstances do not inhibit the inclusion of information supporting that suspicion gathered from within its own corporate group or from another corporate group or entity, including information gathered in these circumstances from outside the jurisdiction in which the report is to be filed.

³ The Financial Action Taskforce, *The FATF Recommendations: International Standards on Combatting Money Laundering and the Financing of Terrorism and Proliferation*; February 2012

⁴ The main issues involved in updating the FATF Recommendations relate to external impediments to information sharing. We would note that many regulations currently prohibit the sharing of SARs and their underlying information. It would be beneficial overall if where a SAR is actually filed, at the very least both the underlying information and the knowledge of the SAR filing are available to be shared across all domains (*i.e.*, enterprise-wide, among financial institutions not part of the same financial group, and between governments and the private sector).

- Countries should ensure that laws relating to the filing of such reports facilitate the filing of identical reports with the Financial Intelligence Unit (“FIU”) in each jurisdiction in which suspicious activity has taken place, or information supporting that suspicion has been gathered.

2. IIF case study: highlighting the challenges and barriers to effective information sharing for the purpose of financial crime risk management

Background:

In order to examine the size and complexity of the challenge to effective information sharing of AML/CFT information, a full and comprehensive review of jurisdictional legal impediments and how they can be addressed is crucial. As an example of the issues involved, the IIF presents this case study in the name of Mundus Bank (“Mundus”), a fictitious representation of a major global banking and financial services organization, with around 3,000 offices in both mature and emerging markets. Financing trade is at the core of Mundus Bank’s business.⁵

Mundus Bank serves around 35 million customers, in 50 countries and territories. Mundus has a presence in each of the jurisdictions represented in this case study, and has correspondent banking relationships in a further 100 countries and territories. High risk business counterparties involved in international trade continue to comprise much of its client base. Mundus’s global footprint and scale mean that it processes two million cross-border transactions each day, and files 100,000 SARs annually.

We emphasize that though this scenario is based on a fictitious bank, the examples themselves are based on real-life situations.

Case Study:

1. Outline of the investigation

The example begins with a Mundus Suspicious Activity Alert, triggered when transaction monitoring identified a pattern of round figure payments into a Mundus account in Singapore. The subsequent Mundus investigation identified the following related trade and transaction flows.

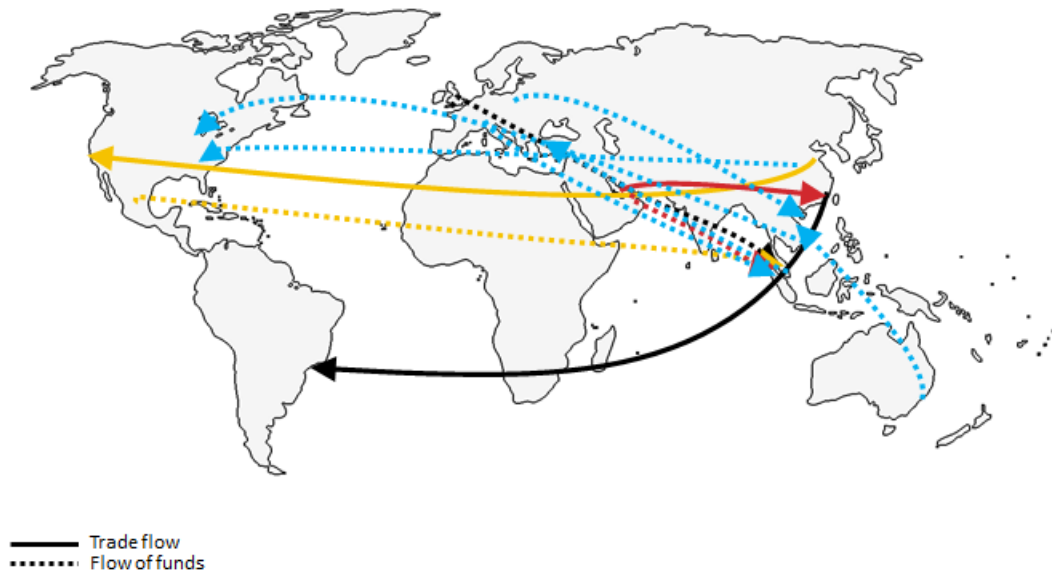
- A Mundus account in Singapore received funds from the United Kingdom (“UK”). The originator was based in Latin America. The payments were for textiles, imported from China to Paraguay. In total, there were 102 payments between December 2013 and June 2014, amounting to USD 5.7m

⁵ This case study makes reference to a number of international jurisdictions. These jurisdictions have been selected to represent the range of challenges presented by their domestic laws, and their selection should not be seen as a criticism or otherwise.

- The same Mundus account in Singapore received funds from an account in Mexico which belonged to an individual. The payments were for electronics, imported to the United States ("US") from China. In total, there were 67 payments between September 2013 and June 2014, amounting to USD 3.3m
- A Mundus account in Dubai sent funds to a second Mundus account in Singapore. The payments were for goods imported to Hong Kong from the United Arab Emirates ("UAE"). There were a limited number of payments, 15 in total in Euros and US dollars. These amounted to EUR 1.5m and USD .5m

Following the flow of funds, Mundus identified a network of accounts including Mundus Bank corporate customers and non-Mundus customers. It identified that some counterparties transacted via relatively small money service businesses and that the network demonstrated little or no normal business activity. It was also marked by indicators of unusual financial activity in multiple jurisdictions.

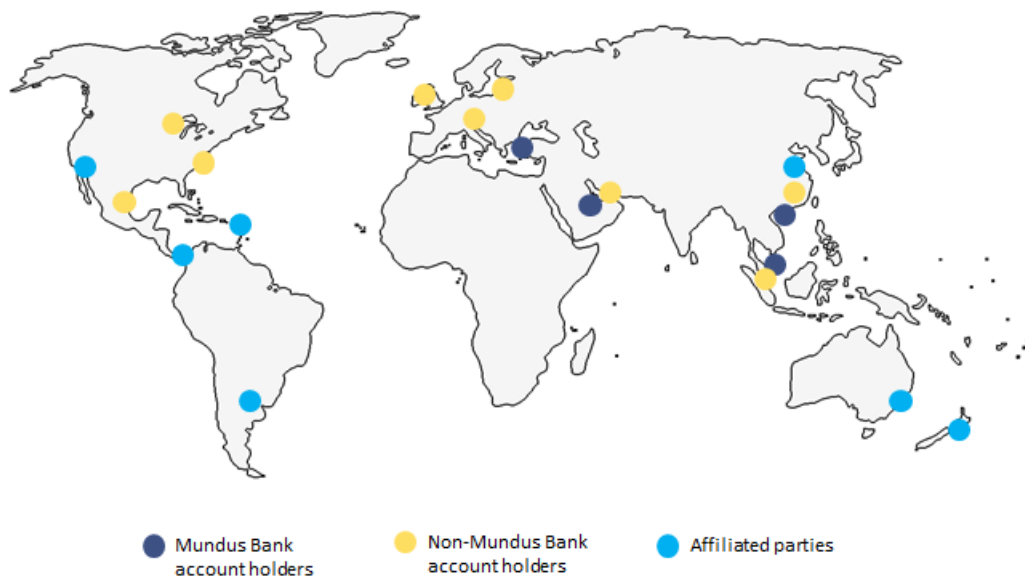
A complex global network used for illicit financial activity



Only four Mundus account holders appeared to be part of this network. They operated in multiple and disparate lines of business. Their Know Your Customer ("KYC") profiles did not identify links to accounts in other jurisdictions. A review of their transactions data identified non-Mundus accounts that played a significant role in the network and they were significant either due to the total funds they transacted to Mundus accounts, and/or because of the frequency of their transactions.

Through a combination of public domain research, closed sources and internal records, it was identified that affiliated parties were located in various jurisdictions and some were in countries with inadequate records of transparency, as documented by international oversight bodies. For example, the true source of funds paid out of the UK Money Service Business (“MSB”) was a Paraguay-based firm, with a nominee director domiciled in Panama. Open sources claimed the nominee director was connected to other companies, however it was impossible to obtain the registration record to confirm the ultimate beneficial owner(s), or the nature of the business. Mundus could not confirm whether the account holder was a front company for illicit financial activity. Similarly, some of the non-Mundus counterparties appeared to be holding companies registered in the British Virgin Islands (“BVI”). As above, it was impossible to determine the ultimate beneficial owners.

Poor transparency in some jurisdictions hinders identification of illicit financial activity



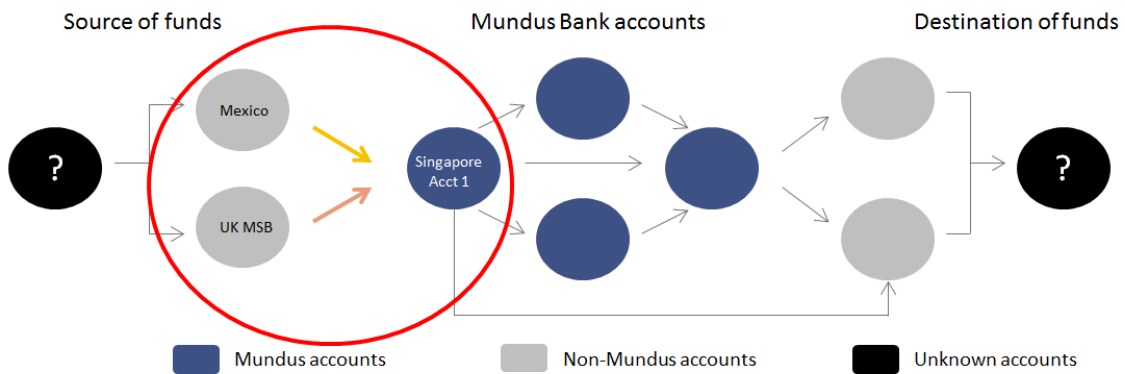
Mundus investigators identified indicators of illicit financial activity, specifically:

- A similar pattern of large round figure payments in common denominations being sent to Mundus Account 1 by an individual in Mexico, and an MSB in the UK on behalf of a company located in Paraguay. The round figure amounts generally ranged from USD 20,000 to USD 200,000. Several of the transactions were just below a round figure, which could indicate that a transaction fee or small percentage had been taken from the payment.
- The MSB making the payment is known to Mundus Bank, because it also featured in a previous investigation into a Mundus account in Hong Kong held by the director of the MSB. The director was investigated after law enforcement provided intelligence suggesting his account was involved in email hacking fraud. The UK investigative arm of

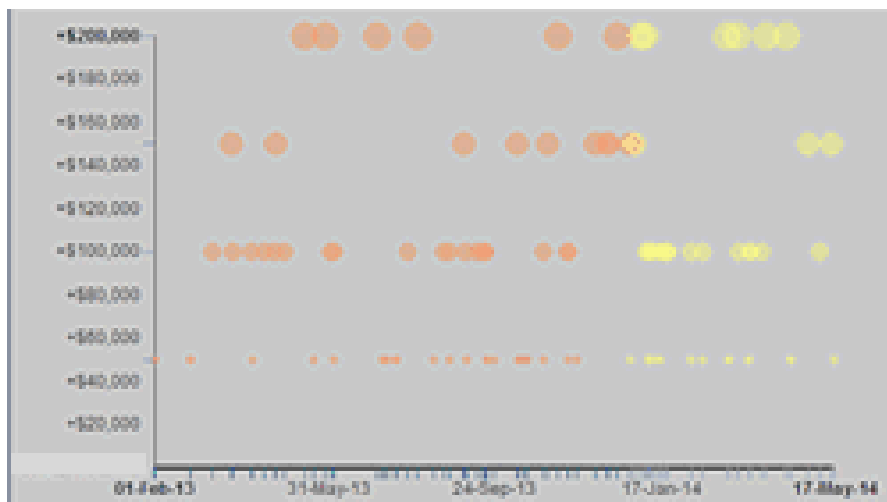
Mundus discovered that the MSB’s director used to be a client of Mundus in another jurisdiction. Internal records showed that there was an internal investigation launched by Mundus Hong Kong. However, the UK team could not view the outcome of the investigation, which was the filing of a suspicious transaction report (“STR”) that ultimately led to the closure of the account. Local data sharing rules do not allow for STRs to be shared outside the jurisdiction. This prevented the formulation of a holistic risk profile of the MSB and to an extent, the network.

A review into the Mundus account in Singapore showed rapid movement of funds from this account into other Mundus accounts in Singapore and Hong Kong. These accounts had been linked to previous internal investigations into money laundering concerns, involving Mundus accounts in Turkey and the UAE. Some of the Mundus accounts in Singapore and Hong Kong were controlled by Australian and New Zealand nationals, who provided addresses in these countries when registering the company.

Observed activity in a global network used for illicit financial activity



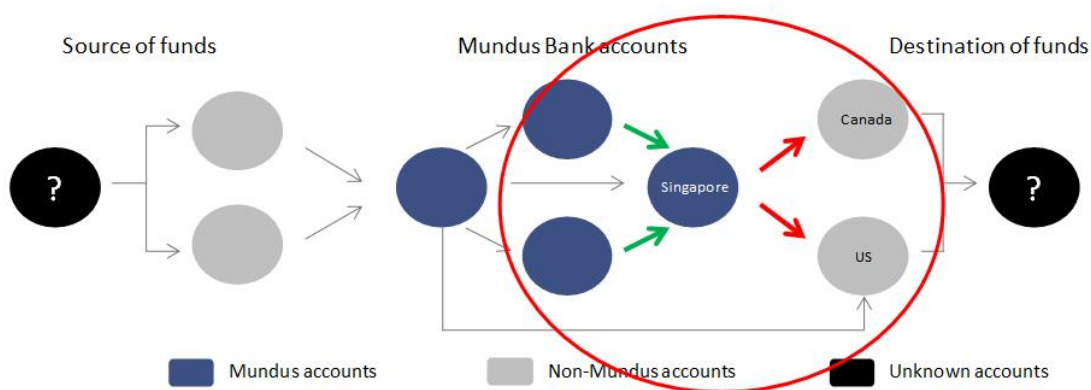
A pattern of large round dollar payments often in succession and in common denominations



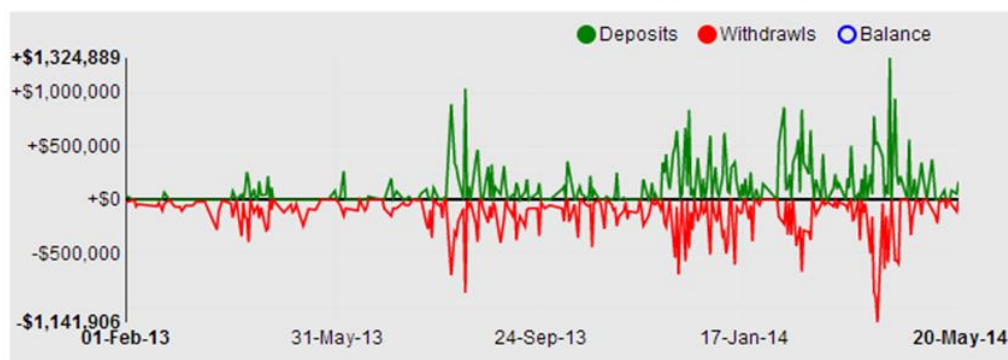
In turn, these accounts appeared to funnel the proceeds from the initial Mundus accounts and a broad range of other accounts into successively higher amounts. This culminated in one Mundus account in Singapore paying USD 24.6m (98.4% of all payments) to several third party accounts in the United States and Canada.

These accounts belong to a company with a latest reported operating turnover of USD 360,000. The director of this company also appears as a director of the company which held the initial Mundus account (Account 1).

Observed activity in a global network used for illicit financial activity



Timeline of deposits into a Mundus account followed by rapid withdrawals from its account to non-Mundus accounts illustrating almost mirror-like activity

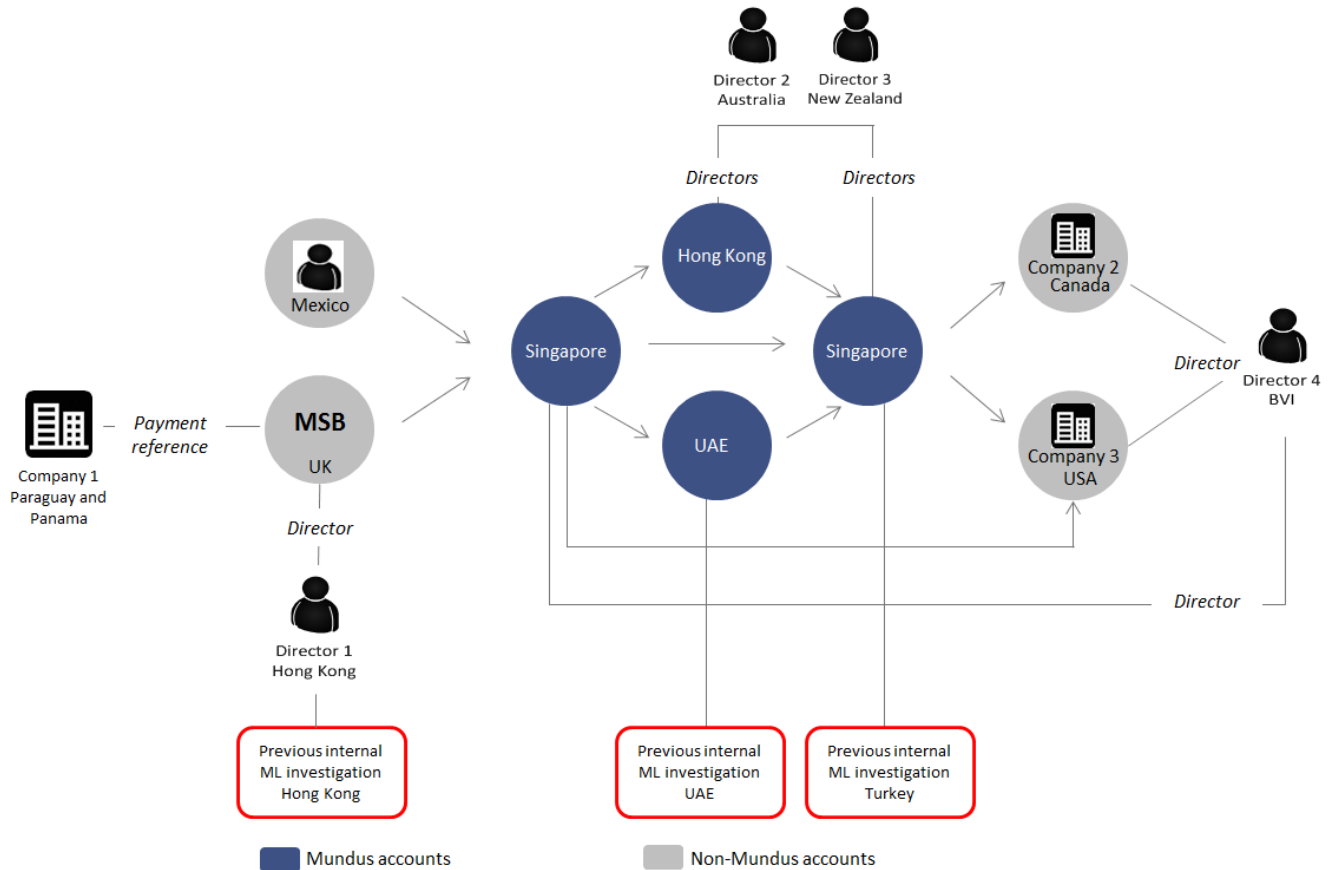


2. Summary of the main issues in the investigation

- Unusual transactions to a Mundus account triggered a system-generated suspicious activity alert.
- Money laundering investigators identified that one of the main sources of funds into the first Mundus account was linked to a previous investigation.
- The investigators identified other Mundus accounts that received funds from the first Mundus account. Several Mundus accounts shared the same nominee directors, located in low-risk jurisdictions. Some accounts had been linked to previous money laundering investigations in Mundus's Turkey and UAE operations.

- The destination of funds from the 'final' Mundus account were non-Mundus accounts located in low risk jurisdictions, apparently operating in incongruent industries. They also shared the same director as the first Mundus account.
- Mundus was unable to determine the original source and ultimate destination of funds.

Mundus' view of illicit financial network



3. Jurisdictional visibility in relation to the investigation

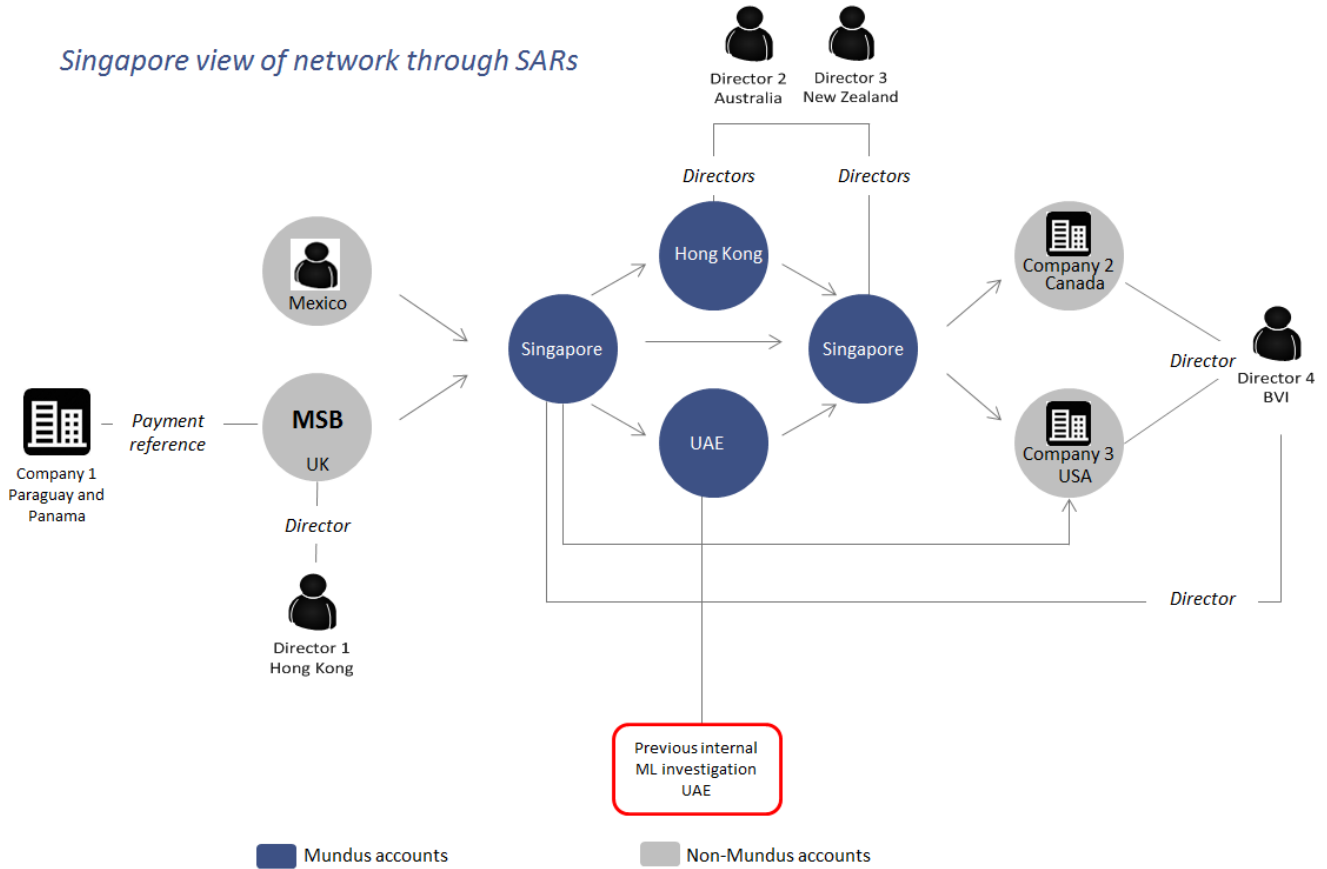
This investigation presents several key examples of jurisdictional visibility, or lack thereof, in how information is shared.

The location in Singapore of the key Mundus accounts at the beginning and end of this money laundering funnel mean that, once SARs have been filed, the Singapore national FIU has the most complete view of the network. Four SARs could be filed: one for the funds coming into the first Singapore account, one for the funds leaving the first Singapore account, one for the funds coming into the second Singapore account, and one for the funds leaving the second Singapore account.

However, even in Singapore, the view is incomplete: data sharing restrictions in Turkey mean that Singapore has no visibility of Mundus Turkey's money laundering investigation of an account linked to the Mundus Hong Kong account in the middle of this network.

Country view of global network used for illicit financial activity

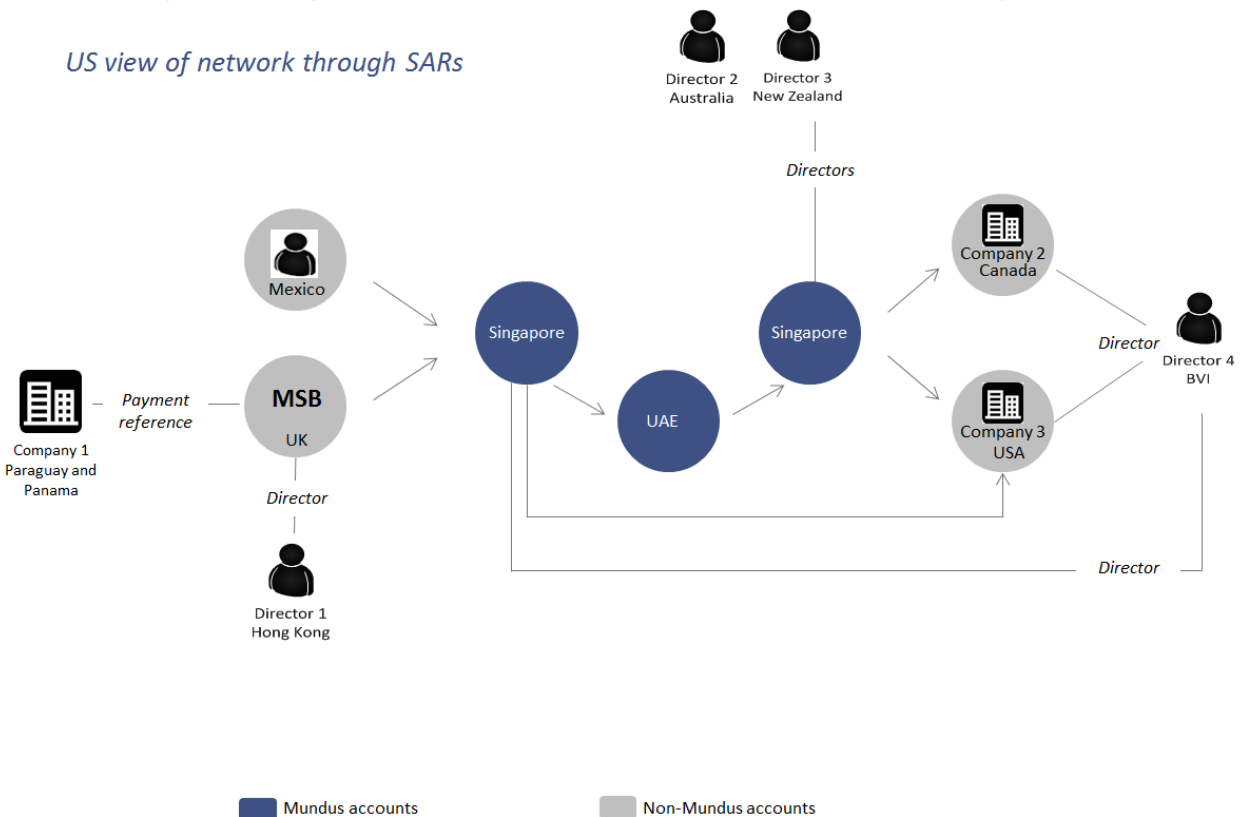
Singapore view of network through SARs



However, the US view is not quite as complete as that of Singapore:

Country view of global network used for illicit financial activity

US view of network through SARs

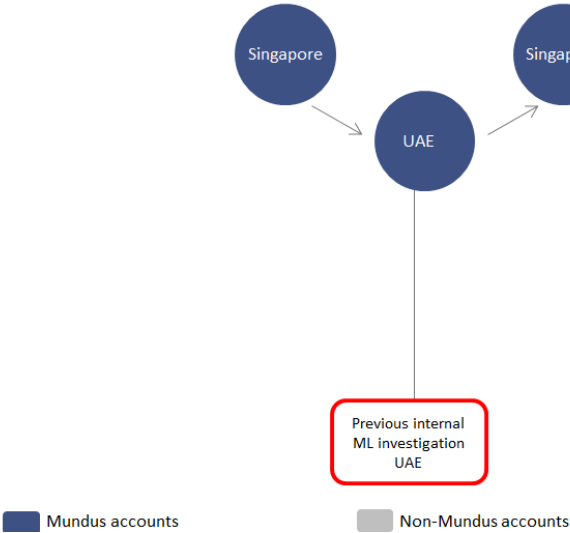


Mundus's policy is that dollar transactions within the Asia Pacific region are cleared through Mundus Singapore. Dollar transactions outside Asia Pacific are cleared through Mundus US. So while the US authorities will have visibility of those parts of the network covered by Mundus US SARs, they will have no sight of USD transactions cleared by Mundus Singapore.

Other jurisdictions have a far less complete view. The UAE will only see the transactions that flow through the UAE account:

Country view of global network used for illicit financial activity

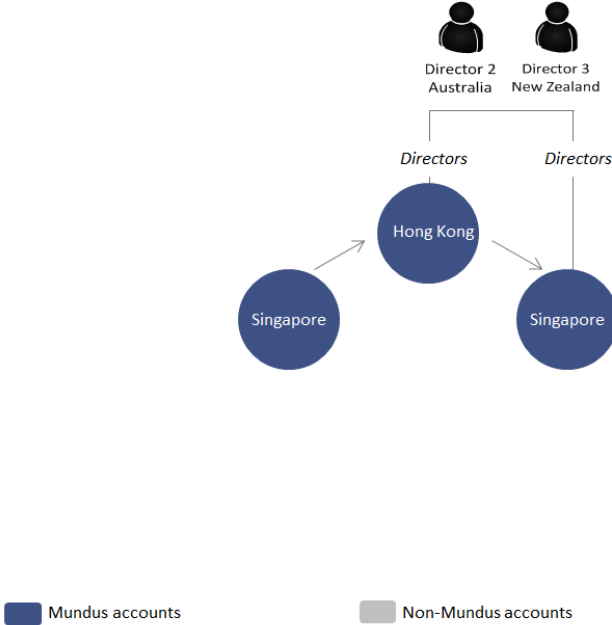
UAE view of network through SARs



Hong Kong's view is similarly restricted:

Country view of global network used for illicit financial activity

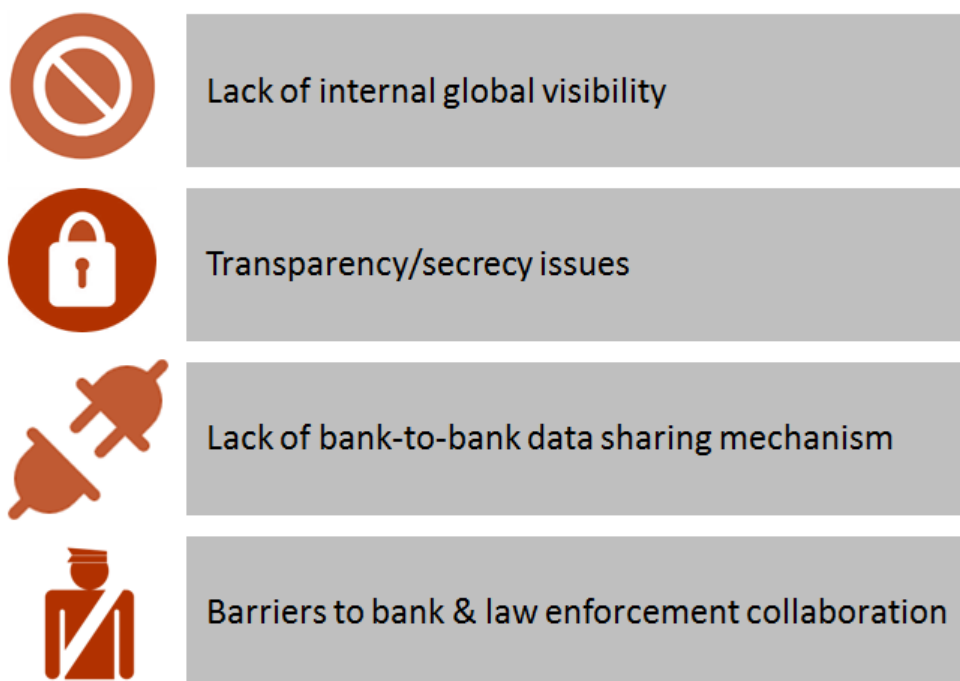
Hong Kong view of network through SARs



The authorities in Australia, Canada, Mexico, New Zealand, Turkey and the UK see nothing. There are no Mundus accounts in these countries, no SARs will be filed there, and so these authorities will have no knowledge of the network.

4. Barriers to a comprehensive view of global networks and collaboration

This case highlights four barriers to effective internal assessment and mitigation of risk, and to collaboration with external parties:



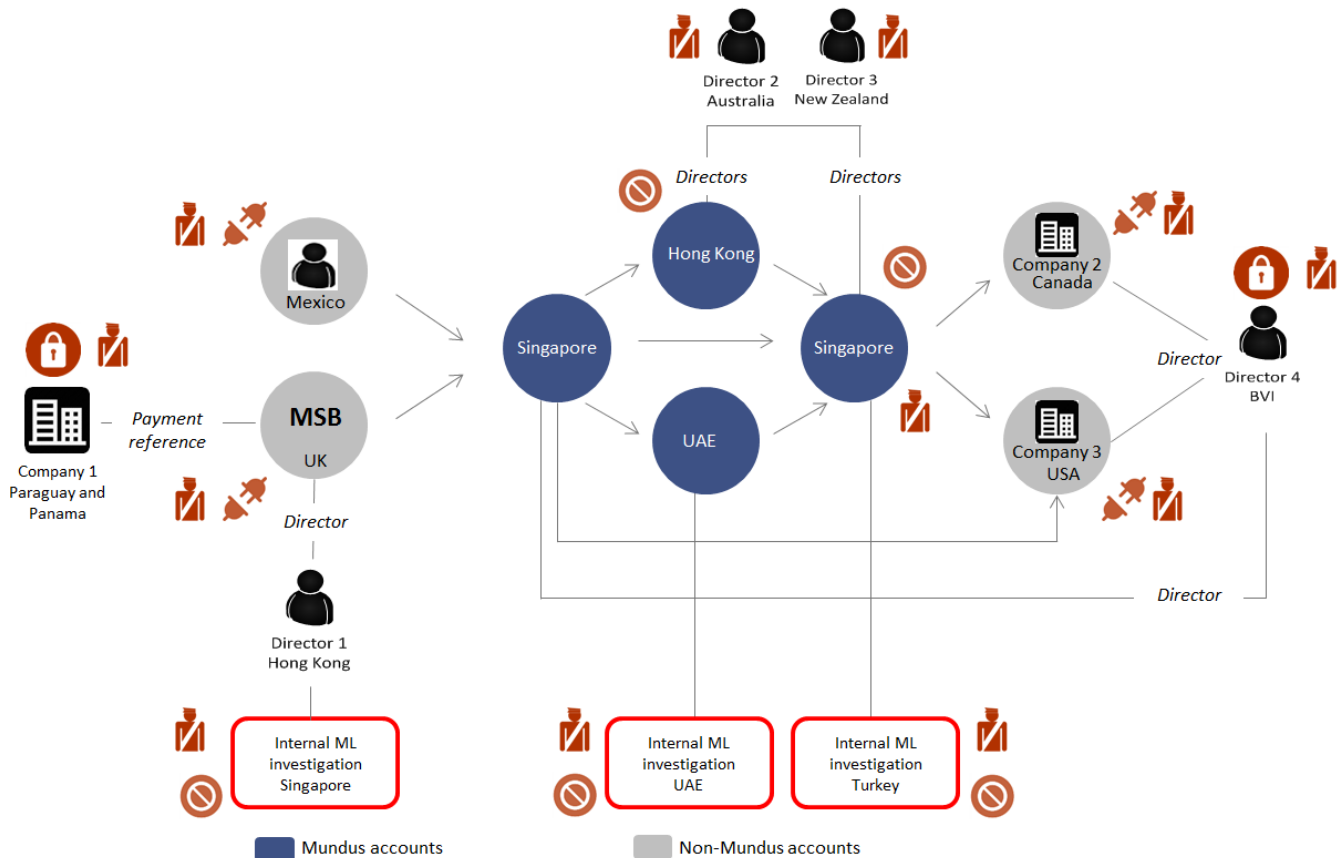
- a. Each Mundus country office has to comply with local data sharing regulations, which prevents the bank establishing a complete picture of a client's global footprint;
- b. A number of jurisdictions have transparency and secrecy issues, which prevent identification of the real people behind the accounts;
- c. Mundus Bank may not discuss identified financial crime risk in non-Mundus accounts with the banks where these accounts are held. This hinders Mundus Bank from finding and following critical illicit financial paths in a large network;
- d. Each jurisdiction files suspicious transaction reports to comply with local filing regulations. Each FIU sees only that part of the network that relates to its jurisdiction: there is no central body that sees all these reports and can communicate with/coordinate the law enforcement response. Where transactions are with non-

Mundus accounts in jurisdictions where Mundus hasn't filed (because there isn't a suspect Mundus account in that jurisdiction) the local FIU and law enforcement will have no visibility of the network at all.

5. Conclusion

This case study outlines the significant barriers to risk assessment, information sharing and collaboration facing the industry, governments and international bodies:

Barriers to a comprehensive view of global networks and collaboration



- Mundus client data in one jurisdiction which includes suspicious activity reporting cannot be shared with another jurisdiction due to local data sharing restrictions.
- Some of the non-Mundus accounts are held with financial institutions located in the EU, but the account holders appear to be holding companies located in off-shore jurisdictions. There is limited open source information on the ultimate beneficial owner and management structure. The same applies for some of the directors based in off-shore jurisdictions. UK-based payment services firms are transacting on behalf of customers based in Latin America, which obscures the true source of funds.

- Mundus Bank has no visibility of where the funds came from, and where they are going to, because it cannot view the transactions of non-Mundus accounts.
- Local regulations mean that STRs/SARs filed by Mundus Bank in different jurisdictions cannot be shared outside the jurisdiction of filing. Only Mundus can truly see the global scale of the network.

In the context of the broader submission on updates to the FATF Recommendations regarding information sharing, the impediments outlined in the Mundus example could be mitigated by allowing more efficient dialogue and more effective information sharing in the enterprise-wide context, among financial institutions not part of the same financial group, and between governments and the private sector.