World Customs Organization

EGMONT GROUP
OF FINANCIAL INTELLIGENCE UNITS

CUSTOMS - FIU COOPERATION HANDBOOK

SANITIZED PUBLIC VERSION

CUSTOMS - FIU COOPERATION HANDBOOK

SANITIZED PUBLIC VERSION

World Customs Organization

EGMONT GROUP OF FINANCIAL INTELLIGENCE UNITS

Acknowledgements

The World Customs Organization (WCO) and Egmont Group of Financial Intelligence Units would like to thank the following individuals for their vision, insight and hard efforts in the conceptualization and creation of the Customs-Financial Intelligence Unit (FIU) Cooperation Handbook (CFCH):

Mr. Nedko Krumov with the Egmont Group Secretariat; Mr. David Kane with the WCO/DHS-Homeland Security Investigations (HSI); Mr. Marko Stolle, Mr. Ulrich Mediger and Mr. Rafael Schneider with the German Customs Service/Germany-FIU; Mr. Endre Banyai and Mr. Gabor Simonka with the Hungary-FIU; and Mr. Jens Christensen with the Denmark-FIU.

The collaborative effort of these eight gentlemen led to the creation of this important anti-money laundering tool and reference source for all Customs Services and FIUs around the world. These gentlemen have designed the CFCH to be a living document that will constantly adapt to the changing global money laundering and terrorism financing environment. May the CFCH continually provide authorities insight and guidance into nuances in methods, trends and technologies that are utilized in the attempt to provide legitimacy to dirty money.

Photo credits: Cover page: © AdobeStock/Andreyphoto63, M.Dörr & M.Frommherz, Tsuboya; Inside pages: © World Customs Organization.

CONTENTS

INTRODUCTION

Over the course of the last quarter century, the advancements in technology, communication, transportation and travel have had a profound, complementary effect on the explosive growth in global commerce. The world has benefited from the increased speed of communication, transport and travel. This growth in global commerce has led to an exponential increase in the volume of financial transactions worldwide, thus enhancing the role of both financial and non- financial entities in the reporting regime for Financial Intelligence Units (FIUs). Consequently, this reality increases the importance of FIUs' dissemination of financial intelligence within the law enforcement community.

The value-added to the global economy through more rapid and efficient trade as well as the higher amount of financial transactions is accompanied, however, by a heightened challenge for Customs services, FIUs and entrusted law enforcement authorities in the form of exploitation by transnational criminal organizations (TCOs) and terrorist organizations. TCOs engage in myriad activities in furtherance of generating illicit revenues, from arms trafficking, narcotics trafficking, general smuggling, customs fraud, embezzlement, IPR fraud, counterfeit food and pharmaceutical fraud, etc. The illicit funds that are generated through these and other criminal activities are the end goal of all TCO activity. The successful laundering of these funds is crucial for TCOs in order to maintain their illegal criminal activities and benefit from the proceeds of crime. Terrorist organizations also regularly smuggle and/or launder their funds across international borders in furtherance of their murderous and destructive agendas.

Although criminal exploitation of the global commercial network represents a small fraction of overall trade, the sheer growth in international trade leads to a corresponding increase in criminal activity and, more importantly, a greater opportunity for TCOs to blend their illicit activities and shipments into the larger, legitimate trade and financial systems. With greater trade volume, the greater the challenge for Customs Services and FIUs to detect illicit shipments and money flows as well as to counteract these illegal activities.

In the same way that automation and technology has increased the speed and efficiency in trade, so must Customs Services and FIUs also use technology and enhanced communication systems to their advantage in combatting TCOs in the trade arena when it comes to countering money laundering (ML), terrorism financing (TF) and the related predicate crimes. Customs and FIUs each have their own in-depth expertise and information sources. However, to identify, disrupt and dismantle TCOs and terrorist organizations, a closer cooperation and specifically the exchange of information and expertise is essential.

It is in furtherance of the global battle to contain this illicit activity that the WCO and the Egmont Group of FIUs conceptualized and created the Customs-FIU Cooperation Handbook (CFCH). The recognition of the need to develop the CFCH was the direct result of the G20 commission to the WCO in 2016, to study the negative effects of illicit financial flows (IFFs) on international commerce. The WCO subsequently approached the Egmont Group and proposed the development of this anti-money laundering (AML) tool. Both organizations supported this idea. The WCO Secretariat presented its intention to develop the CFCH in partnership with the Egmont Group at the 37th session of the WCO Enforcement Committee in March of 2018 and the proposal was endorsed by the WCO membership. The Egmont Group, in turn, presented the concept note for the handbook at its Plenary meeting in Sydney in September of 2018, where it was also endorsed by the Egmont membership.

Shortly after the Egmont Plenary in Sydney, a CFCH Drafting Team was assembled, which included representatives from the WCO Secretariat, FIU Hungary, FIU Germany, and FIU Denmark, also supported by the Egmont Group Secretariat. This team collaborated closely over the course of the ensuing months to design this important AML/CFT document. The WCO and Egmont Group hope that this handbook will provide great benefits to Customs administrations and FIUs alike for many years to come.

In designing and distributing this Handbook, it is the goal of the WCO and the Egmont Group to provide a very practical and current AML/CFT tool and reference guide for all FIUs and Customs Services which will enhance their capacities to combat financial crime and money laundering in the Customs arena. The handbook has also been strategically constructed for FIUs and Customs Services to address Customs-based money laundering in a three-prong fashion: identification, interdiction and investigation. The need to more effectively combat money laundering that touches upon the Customs arena can never be understated, as a heightened capacity for Customs money laundering enforcement will always lead to a commensurate reinforcement of national, regional and international security.

THE ROLE OF THE FIUS AND THE EGMONT GROUP

The primary tasks of the FIUs are the collection of information, the analysis and the assessment of that collected information and ultimately its dissemination to the law enforcement, prosecutorial, other competent authorities and foreign FIUs.

FIUs have a crucial role in the AML/CFT regime. The Financial Action Task Force (FATF), the primary standards setting authority in the field of AML/CFT, adopted its recommendations on combatting money laundering and the financing of both terrorism and proliferation in 2012 and these are updated on a regular basis. According to Recommendation 29, countries should establish a financial intelligence unit (FIU) to serve as the national center for the receipt and analysis of suspicious transaction reports (STRs) and other information[1] relative to money laundering and associated predicate offenses,, as well as activities related to terrorism financing[2]. The FIU should be able to disseminate, spontaneously and upon request, information and the results of its analysis to relevant competent law enforcement and other authorities, and should use dedicated, secure and protected channels for the dissemination of this information.

The primary tasks of the FIUs are the collection of information, the analysis and the assessment of that collected information and ultimately its dissemination to the law enforcement, prosecutorial, other competent authorities and foreign FIUs. The examples of illicit financial activity analyzed by the FIUs are broad in spectrum. Proceed-generating offenses can include drug trafficking, terrorism financing, general smuggling, arms trafficking, tax crimes, various types of frauds, financial-economic crimes, corruption, trafficking in human beings and sexual exploitation, among other crime.

The FATF recommendations also specify the FIUs' access to various data sources[3]. This might include corporate, tax, customs, law enforcement, as well as open source information, depending on the jurisdiction. The roles cited above make the FIUs key information hubs and give them central roles in the AML/CFT operational network.

1 E.g. Currency Transaction Reports (CTRs), Wire Transfer Reports and other threshold-based

2 http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

3 Please see FATF Recommendation 29, and the related interpretative note.

The main role of the Egmont Group is to ensure the proper technical, legal and operational conditions for communication between its members.

Considering that a large proportion of the information analyzed by the FIU have international dimensions, providing a proper framework for the information exchange between foreign FIUs is crucial. In addition to FATF Recommendation 40, the Egmont Principles for Information Exchange between FIUs are considered to be the foundation of international bilateral and multilateral information exchange between FIUs.

The Egmont Group is a united body of 166 financial intelligence units. The main role of the Egmont Group is to ensure the proper technical, legal and operational conditions for communication between its members and to foster the cooperation between FIUs. The primary documents that support the Egmont Group mission are the Egmont Charter and the Egmont Principles for Information Exchange between FIUs[4]. The Egmont documents are designed to be fully in-line with the FATF standards and are binding upon all Egmont Group members. The Egmont documents are considered "soft law", and therefore, violations of these documents are not considered to be violations of international legal obligations; nonetheless, a violation mandates the initiation of non-compliance procedures in an effort to bring the member FIUs in conformity with the Egmont principles.

4 Documents can be downloaded from the Egmont Group website here https://egmontgroup.org/en/document-library/8.

THE ROLE OF THE CUSTOMS SERVICES AND WCO

The Customs Services are uniquely situated to combat money laundering, as they are the tip of the spear with regard to the international movement of illicit goods and products, as well as currency and currency equivalents.

They are the gate-keepers at the international borders, whether they be inland, maritime or external ports of entry. There is great variance among the Customs Services' mandates and investigative authorities vis-à-vis anti-money laundering and counter terrorist financing. Many Customs Services have interdiction authority for undeclared international currency movement or currency transported as part of money laundering schemes. FATF also has specific recommendations regarding cash couriers and detecting the physical cross-border transportation of currency and bearer negotiable instruments through a declaration and/or disclosure system[5]. Some Customs Services also have full investigative mandates to target, initiate and complete money laundering and terrorism financing investigations, such as Homeland Security Investigations (HSI) in the United States and the German Zollkriminalamt, among others.

No matter the extent of the Customs Services' anti-money laundering authorities, almost every Customs Service has an integral role to play in national and international security based on the simple fact that they have the mandate to identify, intercept and seize illicit currency that criminals and criminal organizations attempt to transport across national borders.

The modes of laundering money on the international stage has become increasingly complex in recent years, as technology and methods of monetary transfer have offered criminals both more rapid and alternate means of moving their ill-gotten gains. These methods of laundering money on the international stage vary from the centuries' old scheme of smuggling bulk cash; to the movement of illicit funds within stored value cards; to the conversion of illicit funds into commercial goods and their subsequent integration into international commerce; to the electronic transfer of dirty money via the banking, money remittance business or hawala systems. Other challenging methods for authorities when it comes to the physical movement of ill-gotten proceeds include the movement of assets in the "virtual" realm, which variably can be stored in virtual wallets, mobile devices, personal computers, and other IT hardware.

The WCO is an independent intergovernmental body representing and supporting 183 Customs administrations across the globe that collectively process approximately 98% of world trade. It is a strong international law enforcement proponent in the battle to contain money laundering by TCOs and terrorist organizations. This is demonstrated not only in its ongoing global and regional efforts to combat bulk cash smuggling and trade-based money laundering (TBML), but also through the following anti-money laundering declarations, recommendations and resolutions:

i. Declaration of the World Customs Organization on Transnational Organized Crime (Budapest, 18 June 1997)
ii. Recommendation of the Customs Co-Operation Council on the Need to Develop and Strengthen the Role of Customs Administrations in Tackling Money Laundering and in Recovering the Proceeds of Crime (Brussels, 25 June 2005)
iii. Punta Cana Resolution (Punta Cana, December 2015)

The WCO expertise in countering illicit financial flows (IFFs) has been acknowledged and highlighted by the G20 in the G20 Leader's Communique at the G20 Hangzhou Meetings in September 2016. The G20 also commissioned the WCO to generate an analytical report on IFFs connected to trade mis-invoicing. This report, the Study Report on Illicit Financial Flows via Trade mis-invoicing, was published in 2018. It is a goal of the WCO to increase both the understanding of its Members with regard to money laundering and terrorism financing risks, and improving the expertise and operational successes in combatting the same. The current strategy of the WCO is to make combatting international money laundering and terrorism financing a mainstay in its global enforcement and capacity building efforts. This will be done through capacity building workshops and both regional and global enforcement operations. These operations will be conducted both as WCO stand-alone projects with the respective domestic Customs Services, and as joint operations with its international law enforcement partners, such as INTERPOL, Europol and Frontex.

5 Please see FATF Recommendation 32 and its interpretative note.

THE PURPOSE OF THE CUSTOMS-FIU COOPERATION HANDBOOK

Due to the foregoing, it is the intention of the WCO and the Egmont Group to create this Customs-FIU Cooperation Handbook to assist Customs Services and FIUs in jointly and more effectively combatting the scourge of financial crime, ML and TF.

The aim of this document is to serve as a practical tool for FIUs and Customs Services as well as other law enforcement authorities (such as certain National Police Services) with competences in cross-border related investigations. This Customs-FIU Cooperation Handbook will serve as an orienting guide for those authorities and will address mechanisms and institutionalized practices whereby the Customs Services and FIUs can most effectively collaborate in targeting and dismantling TCOs and terrorist organizations engaging in international money laundering and terrorism financing activities.

This handbook also provides an overview of current challenges and recently identified *modi operandi* that Customs Services and FIUs both face in their continuous fight against ML and TF. Furthermore, it also provides recommended structures to best share financial, customs and other relevant intelligence; recommendations for cross-training and cross-pollination within each other's organization; and the best practices to have in place to combat ML and TF.

COMMON AML CHALLENGES

1. SMUGGLING AND CONCEALMENT OF CURRENCY (BULK CASH SMUGGLING - BCS), CURRENCY EQUIVALENTS, GEMS AND PRECIOUS METALS

DESCRIPTION

The identification, seizure and forfeiture of illicit cash are still some of the main focal points of the authorities tasked with combating ML and TF. TCOs continue to generate large amounts of illicit cash, of which significant portions are used to facilitate and continue their illegal activities.

According to the FATF report on "Money Laundering through the Physical Transportation of Cash" (October 2015)[6] the criminal economy is still overwhelmingly cash-based. The principal attraction and benefit for criminals in the utilization of cash is the fact that it is anonymous, leaves no audit trail and can easily be used/ moved without dependence on technology. Although cash can be smuggled in all the different currencies, the preference for the professional money launderers[7], TCOs and terrorist organizations is to maintain the currency in the form of "hard currency". The widely recognized hard currencies today are the U.S. Dollar, the Euro, the Yen, the British Pound Sterling and the Swiss Franc.

There are various sources for the generation of illicit currency. According to responses generated pursuant to the 2015 FATF report, general smuggling activities rank second on the list of cash generating predicate offences, behind drug trafficking. Tax fraud ranks third in this survey.

There are legitimate causes of cross-border movement of cash especially in those economies which are still cash-intensive, such as in many of the developing countries. However, outside these economies, most law-abiding citizens do not transport large amounts of currency, due to the inherent risk of loss for various reasons. Individuals and organizations that engage in bulk cash smuggling activities most often are doing so because they do not want the responsible law enforcement authorities to become aware that they possess such large amounts of currency.

Customs Services are faced with numerous challenges when it comes to detecting and controlling the cross-border transportation of currency. These challenges are removed from the public summary as they include vulnerabilities that could be exploited by criminals. Furthermore, it is essential for Customs Services to have an effective and efficient working relationship with other pertinent agencies, such as the national police services, when it comes to interdicting, seizing and investigating illicit currency at the borders. The increasing complexities surrounding international money laundering demands that the domestic Customs Services, national police services and FIUs work together in a robust manner to counter this threat to national security and the stability of the financial system. In order to establish seamless cooperation between these agencies, it is important to ensure the alignment of their internal policies.

6 http://www.fatf-gafi.org/publications/methodsandtrends/documents/ml-through-physical-transportation-of- cash.html

7 http://www.fatf-gafi.org/publications/methodsandtrends/documents/professional-money-laundering.html

All Customs Services face challenges in enforcing all categories of smuggling, including the smuggling of currency and currency equivalents, as they have jurisdiction over multiple ports of entry (POEs) within their respective countries. Therefore, they must endeavor to deploy their personnel and resources in the most effective manner. These challenges make the need for risk management and intelligence analysis ever the more important. Therefore ML/TF national risk assessments have a fundamental role in properly addressing cross-border risks, to include currency smuggling. Other strategic analysis should be also conducted in order to properly identify and understand the scope and the intensity of these risks.

FIUs' have the responsibility to analyze suspicious financial transactions within their jurisdiction, including through declarations and or disclosures of physical movement of currency and currency equivalents. Customs Services have an essential role in providing FIUs with relevant information regarding illegal and suspicious cross-border movement of currency, as they are the only entity capable of providing the FIUs with such data.

Closer collaboration between the Customs Services and the FIUs is one of the most expedient manners to bridge gaps in the financial intelligence fields for both services. Both organizations should utilize internally-generated intelligence to target the movement of illicit cash by criminal entities. The regular and timely sharing of information on this phenomenon is a key component to enhanced and more effective targeting by the Customs officers at the designated POEs. Conversely, FIUs stand to benefit from financial intelligence generated by Customs Services concerning suspicious cross-border movement of currency and currency equivalents. Receiving such information, allows the FIUs the opportunity to link the suspicious activity with other suspicious financial transactions identified by the financial industry and other public and private sources (STRs, CTRs, police reports, etc.).

The Handbook provides a number of specific recommendations for each separate *modus operandi* identified below. The main purpose of these recommendations is to provide Custom Services and FIUs with practical guidance on effective cooperation and suggest measures to address the most imminent issues which may jeopardize their AML/CFT activities in areas of common interest. The recommendations are not included in the Public Summary as they are considered sensitive and are strictly aimed at FIUs and Customs activities.

MODI OPERANDI

The most prevalent *modi operandi* used to transport currency comprise:

- concealment by passenger,
- concealment within cargo, vehicles, vessels, and aircraft; and
- concealment by mail.

These *modi operandi* are typically used for the smuggling of currency, currency equivalents (e.g. such as personal checks, official bank checks, money orders, traveler's checks, bearer's bonds, etc.) as well as gems and precious metals. The following are some of most prevalent methods:

1. CONCEALMENT BY PASSENGER

This is the most common method of illicit transportation of currency. Currency can commonly be concealed on the person's body, within the carry-on luggage; within checked-in luggage; and in extreme cases, even internally. The methods of concealment on the person could include: within the clothing; taped to the body; within money belts; within footwear; affixed to the body with panty hose/equivalents; concealed within items that the passenger is carrying with him/her. The methods of transporting the currency within the luggage can vary from simply secreted in the luggage, to false compartment concealment, to secretion within other items. Internal couriers transport the currency within capsules similar to those used by narcotics couriers.

Recommendations for Customs[8]:

The Handbook provides with number of practical recommendations for Customs Services and their officers. Most of these recommendations, by being specifically dedicated to these authorities and of sensitive essence, are not included in this Public Summary. The non-sensitive recommendations are the following:

- Provide the necessary training regime for frontline Customs officers and investigators, to include methods of money laundering connected to the movement of currency, methods of concealment, detection methods and intelligence-based targeting.

8 Considering that this category falls primarily under the mandate of Customs Services, the FIU-related recommendations can be found in the General Recommendations section.

- Ensure that the Customs arrival and departure areas have clear indications of the requirements to declare or disclose the transportation of threshold amounts of currency.
- The Customs Services should also regularly refer to the FATF International Best Practices Guide: Detecting and Preventing the Illicit Cross-border Transportation of Cash and Bearer- negotiable Instruments[9]

2. CONCEALMENT WITHIN CARGO, VEHICLES, VESSELS AND AIRCRAFT

Currency/currency equivalents and gems and precious metals can be concealed within various means of transportation such as cars, vans, trucks, maritime craft vessels, cruise ships, private or commercial aircraft and other conveyances. The methods of concealment within these devices vary from casually stored to very complex methods such as non-factory compartments and switch operated compartments.

With passenger cars, vans, trucks and tractor trailers, the currency and equivalents can be stored in myriad factory-standard locations. With larger conveyances such as aircraft, trains and larger maritime vessels, the modes and opportunities of concealment are even more diverse.

Additionally, certain TCOs rely on the use of containers or other forms of cargo for the transportation of large quantities of currency, currency equivalents and gems and precious metals. The heavy and bulky nature of smuggling very large quantities of the said goods creates a limit for what can be transported by individual couriers or that which can be concealed in smaller vehicles. The detection of such cargo is both intelligence- and physical inspection- driven. Due to the shear logistics, quantities and weight involved, it is an intensive effort of equipment, manpower and man-hours to target and interdict such shipments.

Recommendations for Customs:

The Handbook provides with number of practical recommendations for Customs Services and their officers. Most of these recommendations, by being specifically dedicated to these authorities and of sensitive essence, are not included in this Public Summary. The non-sensitive recommendations are the following:

- Provide robust basic and advanced training on vehicle, vessel, aircraft and conveyance smuggling methods as well as cargo and container smuggling methods for Customs Service management and front-line officers.
- Conduct periodic conveyance-focused field operations targeting currency and currency equivalent smuggling. These operations should include other responsible law enforcement agencies where feasible from a policy and legal authority perspective.
- Provide the FIUs with intelligence generated during customs enforcement events.
- Utilize intelligence derived from FIUs' analysis.

9 http://www.fatfgafi.org/publications/fatfrecommendations/documents/internationalbestpracticesdetectingandprev entingtheillicitcross-bordertransportationofcashandbearernegotiableinstrumentssrix.html

3. CONCEALMENT BY MAIL

Concealment of currency, currency equivalents and gems and precious metals can also be made by means of regular mail and express mail parcels or postal parcels. In such cases, the use of high denomination banknotes is common due to the limited space in most such parcels.

Recommendations for Customs:

The Handbook provides with number of practical recommendations for Customs Services and their officers. Most of these recommendations, by being specifically dedicated to these authorities and of sensitive essence, are not included in this Public Summary. The non-sensitive recommendations are the following:

- Establish and maintain a close working relationship with the national postal services and private express shipment companies. In the event of currency seizures, Customs should provide the information surrounding the identified subject(s) to the FIUs. FIUs and Customs should follow up on the utilization of both the typologies / lists of indicators and the training materials. Annual reminder trainings, no longer than 1-2 days, might be a useful tool to refresh the knowledge, raise awareness and collect feedback from the frontline officers in order to update the typologies, lists of indicators as well as the training materiel.

2. TRADE-BASED MONEY LAUNDERING (TBML)

DESCRIPTION

TBML is a primary threat to the security and prosperity of international trade. TBML is an overarching term for many different ML schemes and is recognized by FATF as one of the primary origin concealment methods for illicit funds. FATF defines TBML as the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origin.

Following this definition, TBML may therefore be undertaken in the form of a single or multiple trade transactions and corresponding financial transactions. The scale and varied nature of global trade and supply chains make them an attractive target for abuse by TCOs. Specifically, jurisdictions that position themselves as international financial and trade centers (i.e. free trade zones), and those which maintain a legal framework favorable for corporate registration, as well as those with beneficial ownership-light company registration requirements can become vulnerable to TBML.

TBML may perhaps even be the most complex form of money laundering. The identification and tracking of illicit currency are difficult tasks in and of themselves. When TCOs or terrorist organizations convert the illicit funds into commercial products, gems and precious metals, food products or other marketable items, and subsequently introduce them into global commerce, the investigator's task becomes ever more challenging.

The challenge for analysts and investigators is to link the commercial activities/fraudulent commercial activities with the predicate crimes that generate the illegal proceeds in the first place. The concerted efforts of the FIUs and the Customs Services are an invaluable tool to identify and combat such intricate criminal activity. The FIUs are customarily the primary authority for identifying suspicious financial activities occurring within the banking and financial services sector, while Customs services are the primary authority for identifying commercial anomalies and suspicious commercial activities.

Considering the complexity and different forms of TBML, a short overview of its prevalent techniques / *modi operandi* as practiced in international business is contained below. It must be noted that the criminal schemes listed below can simply occur as customs fraud violations in and of themselves, as well as in furtherance of TBML. The FATF and Asia Pacific Group on Money Laundering (APG) have published some extensive documents on TBML, as well.[10]

MODI OPERANDI

1. FRAUDULENT INVOICING OF GOODS AND SERVICES

Fraudulent invoicing requires a conspiracy between an importer and an exporter. This initially inconspicuous trade relation is misused as the basis for movements of a commercial nature and the laundering of the illicit funds via the subsequent financial transactions. The key element of this technique is the misrepresentation of the price, quantity or type of merchandise in order to transfer additional value between the importer and exporter.

1.1. Over-invoicing / Under-shipment

By invoicing the goods at a quantity above what is actually contained in the shipment, the exporter is able to receive additional value from the importer, as the payment for the goods is more than the value actually shipped. This scheme also allows the commingling of illegal proceeds with legitimate proceeds.

1.2. Under-invoicing / Over-shipment

By invoicing the goods at a quantity below what is actually contained in the shipment, the exporter is able to transfer value to the importer, as the payment for the goods will be lower than the value actually shipped.

Over-invoicing and under-invoicing might be carried out as stand-alone transactions, but these schemes can also be employed in a series of shipments involving the transfer of goods through multiple countries. These schemes can be conducted in furtherance for tax/duty fraud and ML/TF.

1.3. Over-valuation of goods

Through the over-valuation of goods, the exporter and the importer conspire to artificially inflate the value of the goods in question. Through this scheme, the importer is enabled to transfer additional funds to the exporter.

1.4. Under-valuation of goods

Through the under-valuation of goods, the exporter and the importer conspire to artificially deflate the value of goods. Through this scheme, the exporter transfers additional value to the importer

1.5. Invoice reuse

In a fashion similar to the multiple invoicing scheme, the same invoice may be illegally reused on multiple occasions in order for the importer to transfer additional funds to the exporter in excess of the value of the actual shipment. The same invoice can also be used as a mask for multiple shipments of product, without Customs authorities becoming aware.

1.6. Multiple invoicing of goods

Through multiple invoicing schemes, the exporter and the importer conspire to create one or more fictitious invoice(s) connected to one specific shipment. In this manner, the exporter receives excess funds beyond the value of the actual shipment, through two or more associated financial transactions.

1.7. False declarations / False Invoicing

The misdeclaration of goods and services is another relevant technique used for fraudulent commercial activity and ML/TF.

The importer and the exporter can conspire to falsely declare the goods being shipped as being a more or less expensive product or good. By falsely declaring the product as an item of lesser value, the importer realizes the receipt of additional value. On the other hand, by falsely declaring the product of higher value than it actually is, the exporter realizes the receipt of additional value.

10 FATF Trade Based Money Laundering 2006 (http://www.fatf- gafi.org/publications/methodsandtrends/documents/trade-basedmoneylaundering.html)
FATF Best Practices on Trade Based Money Laundering 2008 (http://www.fatf-gafi.org/publications/fatfrecommendations/documents/bestpracticesontradebasedmoneylaundering.html)
FATF Asia/ Pacific Group Trade-based money laundering typologies 2012 (http://www.fatf- gafi.org/publications/methodsandtrends/documents/trade-basedmoneylaunderingtypologies.html)

2. BROKER-RELATED TBML SCHEMES, SUCH AS THE BLACK-MARKET PESO EXCHANGE

Certain elaborate TBML schemes involve the pivotal role of dirty money brokers, customs brokers and middlemen. One such system is the Black-Market Peso Exchange (BMPE) which was put in place to launder the Colombian cocaine cartel drug proceeds in the United States in the late 1970s and 1980s. The BMPE involves the conversion of cash proceeds from cocaine sales to commercial products. The reason for the creation of the BMPE was because of the sheer amount of illicit cash that was generated (millions of U.S. dollars) from this illicit activity. The volume became so large that it became of high risk for the cartels to continue to handle the money laundering side of the business. They then began employing the services of middlemen and money brokers who employed a specialty service in the money laundering process. Money brokers often employ many individuals responsible for collecting narcotics proceeds and disposing of those proceeds, as directed by either the drug trafficking organization or the money brokers who serve as professional money launders[11].

For a designated fee, these brokers took on the responsibility of collecting the dirty cash from designated locations in the United States, usually major cities. Upon collection of the funds, the brokers would take on the responsibility of the remainder of the laundering process. They ensured that the money would either enter the financial system disguised as legitimate commercial activity or directly purchase commercial products with the dirty cash. After the purchase of the commercial products, the BMPE brokers arrange for the export of the products to Colombia or other designated countries. The products are then sold in those countries and obtain the appearance as being part of legitimate commerce. In the case of the products that are shipped to Colombia and sold there, the funds are converted to Colombian pesos automatically and the full circle of the money laundering continuum is achieved. In the cases of products that are sold in third countries, the money can be held in other cartel-controlled accounts in those countries or converted to pesos and transferred to Colombia.

This phenomenon is not isolated to the U.S., but rather to all the primary markets for cocaine. Other criminal organizations that generated large volumes of illicit cash have since adopted this system and are currently employing. Certain criminal hawala systems are known to function in the role of brokers and transfer systems in furtherance of this scheme.

These dirty brokers/brokerage firms have to handle very large volumes of cash in furtherance of the scheme and are hence vulnerable to detection by reporting mechanisms. The marrying of suspicious financial reports with suspicious commercial activity is an ideal method for detecting such nefarious activity, as well. Hence, the collaboration of the FIUs and Customs Services is crucial in combating this phenomenon.

Recommendations for FIUs and Customs services:

The Handbook provides with number of practical recommendations for Customs Services, FIUs and their officers. Most of these recommendations, by being specifically dedicated to these authorities and of sensitive essence, are not included in this Public Summary. The non-sensitive recommendations are the following:

- Through formal collaboration and information sharing between the FIUs and Customs Services, the FIUs, in accordance with the respective domestic legal framework and in line with the general principle of the FIUs' operational independence and autonomy, are encouraged to provide financial intelligence to Customs Services with regard to suspected TBML activity.
- Customs Services are encouraged to conduct further analysis of this information in an effort to link the FIU data to iterative steps in the money laundering/terrorism financing process.
- Due to the complexity of TBML schemes and the possible high volume of transactions involved, both the FIUs and Customs Services are encouraged to establish robust anti- money laundering and TBML training components into their training regimes. They are encouraged to conduct cross-training programs, as well.

11 http://www.fatf-gafi.org/publications/methodsandtrends/documents/professional-money-laundering.html

- The creation of a specialized unit dedicated to addressing such TBML schemes, such as a cargo analysis team or financial investigations unit, might prove beneficial. The Trade Transparency Unit (TTU)[12] is an example of a more advanced cargo analysis unit, whereby import and export data between independent Customs Services are shared in a cooperative basis in furtherance of a bi-lateral agreement. Involvement of FIUs in such specialized units, or the operational cooperation with FIUs if direct involvement is not possible, should be considered as well.
- Conduct robust joint public outreach programs to the general public, freight forwarders, financial companies, shipping companies, brokers, etc. regarding TBML and Customs fraud schemes.
- Customs Services and FIUs are encouraged to engage and outreach efforts with other law enforcement counterparts, to include the prosecutorial authorities, in order to heighten awareness of such schemes amongst all relevant stakeholders.

12 https://www.ice.gov/trade-transparency

3. MONEY OR VALUE TRANSFER SYSTEMS AND ALTERNATIVE REMITTANCE SYSTEMS

DESCRIPTION

The primary electronic monetary transfer systems within the banking industry involve a formalized and well-documented movement of funds. They are transferred between one or more institutions and the actual transaction is settled through a pre-established credit-debit system between the institutions.

This procedure often involves the use of correspondent banks and the support of the messaging services of the Society for Worldwide Interbank Financial Telecommunications (SWIFT), the Clearing House Interbank Payments System (CHIPS) and the Fedwire Funds Service (Fedwire) transfer service system.

The SWIFT, CHIPS and Fedwire services are the industry standard and are widely regarded as the most trustworthy services for domestic and international transfers of funds[13]. There are also other domestic real-time gross payment systems (RTGPs); please see Annex for a listing of some of these systems. Other established corporate money remittance services, such a Western Union and Money Gram, are also commonly regarded as trusted and efficient means of transferring funds, both domestically and internationally.

Money or value transfer systems (MVTS) refers to financial services that involve the acceptance of cash, cheques, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs. Transactions performed by such services can involve one or more intermediaries and a final payment to a third party, and may include any new payment methods. Sometimes these services have ties to particular geographic regions and are described using a variety of specific terms, including hawala, hundi, and fei-chen; often referred to as alternative remittance systems (ARS) are transfer systems that exist exclusively or partially outside of the regulated financial sector.

MVTS include hawala systems, unregulated courier services and exchange houses, as well as certain e-currency transfer schemes, among other methods. MVTS can also include systems involving value transfer via conversion of proceeds to another method of value retention, from gems and precious metals to electronic storage devices, and their subsequent movement from one point to another.

ARS is not necessarily illegal, and these systems often serve as convenient and readily accessible transfer means for communities that do not have easy access to the more well- established, industry standard financial transfer services. However due to the extensive anonymity embedded into ARS, these systems are often misused to transfer illicit proceeds and, therefore, pose a serious anti-money laundering challenge to regulatory and law enforcement authorities.

13 Note: SWIFT is an international system, while CHIPS and Fedwire are domestic transfer systems within the United States.

1. HAWALAS

The most prominent example for ARS is the hawala system. Hawalas tend to be closed-circuit businesses that are often run by families or within tightly-knit, ethnic-based groups. Most hawalas do not engage in criminal activities, but the hawalas that do engage in criminal activities are very difficult for law enforcement authorities to investigate due to the fact that they tend to be internalized businesses. A hawala system operates via the use of two or more branches that are controlled by individuals known as "hawaladars."

The hawala system functions as a credit-debit system, where the accounts are simply settled via on-hand accounts in the control of each hawaladar. Multiple currencies can be used in such a system and for the system to function properly, each hawaladar must have adequate "demand currencies" in his/her possession to fulfill the transactional obligations to their clients. The hawaladars simply settle their accounts between each other post-facto, after the consummation of the clients' transaction.

The hawala system is the most anonymous MVTS in existence, as the funds are neither physically transferred nor electronically cleared from one financial institution to another via a formal wire transfer service.

In its simplest form, it involves two hawaladars (branches or dealers) that operate in two different countries. When a client approaches hawaladar 1 in country A and requests the transfer of $100,000 (U.S.) to his intended recipient in country B, hawaladar 1 provides the client with a unique code that is not commonly in the form of a formal receipt. Hawaladar 1 also provides the contact information for his partner, hawaladar 2, in country B. The client then needs to provide this unique code to his intended recipient, who then approaches hawaladar 2 and receives the $100,000 directly, minus the previously-agreed-to service charges.

Although hawalas can be as simple as a system containing two hawaladars, they more commonly contain a network of hawaladars operating in different countries and cities within countries.

The hawala system can commonly consummate a transfer in a matter of minutes and even simultaneous to the deposit by the initiating client. The reason for the speed of service is that there is not an associated electronic transfer of funds or electronic clearance system that needs to be utilized, as would be necessary with the SWIFT, CHIPS and Fedwire services, for example.

On the other hand, hawaladars occasionally must transfer funds between each other at a future point in order to balance their accounts. This can involve direct electronic transfers between them, the transportation of currency between them, or even the transfer of merchandise or other items of value (i.e. gems and precious metals, etc.) between them.

The FIUs are faced with the challenge that, under regular circumstances, it is very difficult to detect hawala activity based solely on information gathered via the reporting regime. Often, additional information from multiple sources is required to establish that the persons or entities involved are operating a hawala system.

Nonetheless, FIUs are strategically placed to detect potential hawala activities.

Although most Customs Services do not have a mandate to enforce illicit electronic funds transfers, they are ideally placed to intercept smuggled currency and currency equivalents (to include gems and precious metals). They are therefore uniquely placed to detect hawalas that utilize couriers.

2. CURRENCY EXCHANGE HOUSES

Another example of MVTS commonly used by TCOs are currency exchange houses. Although the great majority of these establishments are legitimate and regulated businesses, their cash-intensive structure makes them ideal entities to disguise the movement of illicit proceeds.

Currency exchange services that engage in money laundering activities can also function as MVTS, due to their very similar operational structure. They handle large amounts of cash; they often have multiple branches in different cities; and they have readily available bank accounts to transfer money through. Like hawalas, the currency exchange houses are a common establishment in cash intensive/cash economy regions such as the Middle East and Africa.

3. OTHER METHODS OF VALUE RETENTION AND TRANSFER

The digital age has also ushered in a new panoply of value storage and value transfer methods, as well. This includes: e-currency, electronic storage devices, e-wallets and stored value cards (SVCs), among other methods. E-currency, electronic storage devices, e-wallets and SVCs have two things in common: they are digital/machine-based forms of storing money and in most countries, they are not currently subject to currency and monetary instrument reporting requirements upon transportation into and out of country. The criminal use of such methods to store and move funds is a challenge for law enforcement and regulatory authorities. In order to detain, seize and forfeit dirty money, the law enforcement authorities must first be able to detect it. E-currency can be stored in virtual wallets and virtual accounts. Money can now be stored in cellphone-based technology and electronic storage devices. Upwards of a couple of hundred thousand dollars can be stored electronically on certain SVCs.

Customs officers stand at the forefront in detecting the movement of physical cash. They also stand in the ideal position for detecting the movement of large quantities of SVCs, whether or not they have seizure authority. It should be noted, that where legislation and policy allow, Customs and other law enforcement officers can utilize electronic recovery and access to data (ERAD) devices to determine the amount of funds on the SVCs, in furtherance of criminal suspicion/investigations.

The collaboration between Customs and FIUs can potentially identify and target criminals and criminal organizations that are moving illicit moneys across international borders via stored value cards. The FIUs are at the forefront of such efforts, as their relationship to the financial industry and their access to STRs/SARs would be the primary means of detecting suspicious activities involving the international movement of funds via SVCs. Customs Services and FIU investigation of such activities should be conducted with the support of the national police services and/or other responsible law enforcement agencies in cases where the Customs Service does not have an independent money laundering investigations mandate.

The conversion of currency to other liquid forms of value retention, such as gems and precious metals, is another common method of engaging in MVTS. This method has been covered in the TBML section, but it is worth mentioning in this section as well because TBML is also an MVTS. The high liquidity and easy marketability of gems and precious metals or stones, such as gold and diamonds, make them ideal substitutes for illicit cash. Gems and precious metals also do not generate the alert of currency detection canines and they are both extremely lightweight and easy to conceal.

Recommendations for FIUs and Customs Services:

The Handbook provides with number of practical recommendations for Customs Services, FIUs and their officers. Most of these recommendations, by being specifically dedicated to these authorities and of sensitive essence, are not included in this Public Summary. The non-sensitive recommendations are the following:

- Customs Services and FIUs are encouraged to establish basic training and other supportive training structures for their management and frontline officers to further general awareness of MVTS activities. This training should include specific guidance on what to look for when they encounter possible currency smuggling connected to this phenomenon. The Customs Services must remember that often, they are the eyes and ears for many other investigative agencies with regard to illicit cross-border movement of currency/currency equivalents.
- With regard to Customs Services, the training should provide possible indicators of money couriers and transfer system activity.
- The FIUs and Customs Services are encouraged to collaborate, in accordance with the respective domestic legal frameworks and in line with the general principle of the FIUs' operational independence and autonomy, in efforts to target complicit MVTS/hawalas that are suspected of illicit activity.

RESULTS IN SUMMARY AND CONCLUSIONS

The project group came to the realization that the replying jurisdictions are applying two main approaches concerning operational cooperation between FIUs and customs authorities.

One approach involves the establishment of the cooperative framework and associated guidelines to be laid down in the domestic AML/CFT Act and related government or ministerial decrees/policies. In this model, the regulations were not always strictly limited to the issue of operational cooperation, but in some instances also included the issues of joint or mutual training and mutual secondment programs, among other forms of collaboration.

In the second approach to operational cooperation, which applies to a large group of jurisdictions, joint cooperation is addressed by memoranda of understanding (MoUs) or other bilateral cooperation agreements between the agencies. In some cases, technical committees or working groups have been established to support the effective collaboration.

The Customs Services and the FIUs traditionally represent two of the primary four enforcement pillars to counter money laundering, financial crime and terrorism financing activities around the globe. The other two pillars are the National Police Services (or equivalent) and the prosecutorial authorities.

Customs is the primary sentinel for combatting such activities as they relate to the international border areas. There is no better placed law enforcement authority to counter the illicit smuggling of currency/currency equivalents, gems and precious metals and illicit money on stored value cards and similar media than Customs. Customs Services have specialized detection capabilities in this regard and have their internal databases and information on cross-border transportation of currency to utilize in furtherance of these efforts.

The FIUs are the central authorities for the monitoring of all derogatory financial information connected to possible money laundering, terrorism financing or general financial crime. The FIUs traditionally have a much broader view over the movement of illicit moneys within the national borders, as they receive STR and CTR reporting from the banking industry, financial services industry, real estate industry, other cash intensive businesses and other designated non- financial businesses and professions. In this sense the FIUs are uniquely positioned closer to the reporting entities and can easily obtain, analyze and disseminate financial intelligence to the other competent authorities.

The close collaboration between Customs and FIUs becomes a force-multiplier for national security vis-à-vis illicit financial and money laundering activities. Such collaborative efforts are vital to the overall law enforcement mandate to contain ML and TF, as they automatically enhance the national and economic security of their respective nations.

One of the primary aims of this Handbook is to emphasize and promote this cooperation as a mechanism for more effective disruption of cross-border money laundering and terrorism financing activities. Through joint efforts, the FIUs and Custom Services can more effectively combat the scourge of transnational organized crime and terrorism and they serve as joint protectors of the global financial system and enhance national security for all nations.

The transnational criminal organizations and terrorist organizations have deep pockets courtesy of their illicit activities and they will continue to exploit the bourgeoning spectrum of technologies and methods to move their ill-gotten gains. The robust, joint collaboration of Customs Services and FIUs provides all nations with their most serious weapon to identify, disrupt and dismantle the activities by such nefarious actors at the international borders.

GLOSSARY OF ACRONYMS

AML	Anti-money laundering
ARS	Alternative remittance systems
APG	Asia Pacific Group on Money Laundering
BMPE	Black Market Peso Exchange
BCS	Bulk Cash Smuggling
CDD/KYC	Client Due Diligence/Know Your Customer
CFATF	Caribbean Financial Action Task Force
CFCH	Customs-FIU Cooperation Handbook
CHIPS	Clearing House Interbank Payments System
CFT	Counter-financing of terrorism (can also be referred to as CTF – Counterterrorism Financing)
CTR	Currency transaction report
EAG	Eurasian Group
EBC	Egmont Biennial Census
ERAD	Electronic recovery and access to data
ESAAMLG	Eastern and Southern African Money Laundering Group
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
FSRB	FATF-style Regional Body
FX	Foreign Exchange
GABAC	Central African Anti-money Laundering Group
GAFILAT	Latin American Anti-money Laundering Group
GIABA	Inter-Governmental Action Group against Money Laundering in West Africa
HSI	Homeland Security Investigations
IEWG	Information Exchange Working Group
IFFs	Illicit financial flows
MENAFATF	Middle East and North Africa Financial Action Task Force
ML	Money laundering
MONEYVAL	Council of Europe Anti-money Laundering Group
MoU	Memorandum of understanding
MVTS	Money or value transfer systems
POE	Port of entry
RTGS	Real-time Gross Payment Systems
RTA	Regional trade agreement
STR	Suspicious transaction report (can also be referred to as SAR: Suspicious Activity Report)
SVC	Stored value card
SWIFT	Society for Worldwide Interbank Financial Telecommunications
TBML	Trade-based money laundering
TCO	Transnational criminal organization
TF	Terrorism Financing
WCO	World Customs Organization

ANNEX

REAL-TIME GROSS PAYMENT SYSTEMS (RTGS) FOR INDIVIDUAL COUNTRIES

Albania	RTGS
Angola	SPTR, (Sistema de pagamentos em tempo real)
Argentina	MEP (Medio electrónico de pagos)
Azerbaijan	AZIPS (Azerbaijan Interbank Payment System)
Australia	RITS (Reserve Bank Information and Transfer System)
Bahrain	RTGS [22] (Real Time Gross Settlement (RTGS) System)
Bangladesh	RTGS (Bangladesh Bank Payment Service Division)
Barbados	Central Bank Real Time Gross Settlement System (CBRTGS)
Bosnia and Herzegovina	RTGS
Belarus	BISS (Belarus Interbank Settlement System)
Bulgaria	RINGS (**R**eal-time **In**terbank **G**ross-**s**ettlement System)
Brazil	STR (Sistema de Transferência de Reservas)
Canada	LVTS (Large Value Transfer System) (This is actually an RTGS *Equivalent* system. Final settlement happens in the evening.)
China	China National Advanced Payment System ("CNAPS") (also called "Super Online Banking System)
Chile	LBTR/CAS (Spanish: *Liquidación Bruta en Tiempo Real*)
Croatia	HSVP (Croatian: *Hrvatski sustav velikih plaćanja*)
Czech Republic	CERTIS (Czech Express Real Time Interbank Gross Settlement System)
Denmark	KRONOS
Egypt	RTGS
Eurozone	TARGET2 (Used by a number of countries)
Fiji	FIJICLEAR
Hong Kong	Clearing House Automated Transfer System (CHATS)
Hungary	VIBER (Hungarian: *Valós Idejű Bruttó Elszámolási Rendszer*)
Georgia	GPSS (**G**eorgian **P**ayment and **S**ecurities **S**ystem)
India	RTGS
Indonesia	Sistem Bank Indonesia Real Time Gross Settlement (BI-RTGS)
Iran	SATNA (Real-Time Gross Settlement System)
Iraq	RTGS (Real Time Gross Settlement System)
Israel	Zahav
Japan	BOJ-NET (Bank of Japan Financial Network System)
Jordan	RTGS-JO]
Kenya	Kenya Electronic Payment and Settlement System (KEPSS)
Korea	BOK-WIRE+ (The Bank of Korea Financial Wire Network,)
Kuwait	KASSIP (Kuwait's Automated Settlement System for Inter-Participant Payments)

Lebanon	BDL-RTGS (Real Time Gross Settlement System)
Macedonia	MIPS (Macedonian Interbank Payment System)
Malawi	MITASS (Malawi Interbank Settlement System)
Malaysia	RENTAS (Real Time Electronic Transfer of Funds and Securities)
Mauritius	Mauritius Automated Clearing and Settlement System (MACSS)
Mexico	SPEI (Spanish: *Sistema de Pagos Electrónicos Interbancarios*)
Morocco	SRBM (Système de règlement brut du Maroc)
Namibia	NISS (Namibia Inter-bank Settlement System)
New Zealand	ESAS (Exchange Settlement Account System)
Nigeria	CIFTS (CBN Inter-Bank Funds Transfer System)
Pakistan	RTGS (Real Time Gross Settlement System)
Peru	LBTR (Spanish: *Liquidación Bruta en Tiempo Real*)
Philippines	PhilPaSS
Poland	SORBNET
Qatar	QPS [21] (Qatar Payment System (QPS)
Russia	BESP system (Banking Electronic Speed Payment System)
Romania	ReGIS system
Saudi Arabia	(Saudi Arabian Riyal Interbank Express) SARIE
Singapore	MEPS+ (MAS Electronic Payment System Plus)
South Africa	SAMOS (The South African Multiple Option Settlement)
Spain	SLBE (Spanish: Servicio de Liquidación del Banco de España)
Sri Lanka	LankaSettle (RTGS/SSSS)
Sweden	RIX (Swedish: *Riksbankens system för* överföring *av kontoförda pengar*)
Switzerland	SIC (Swiss Interbank Clearing)
Taiwan	CIFS (**C**BC **I**nterbank **F**unds Transfer **S**ystem)
Tanzania	TIS (Tanzania interbank settlement system)
Thailand	BAHTNET (**B**ank of Thailand **A**utomated **H**igh value **T**ransfer **Net**work)
Turkey	EFT (Electronic Fund Transfer)
Ukraine	SEP (**S**ystem of **E**lectronic **P**ayments of the **N**ational **B**ank of **U**kraine)
United Kingdom	CHAPS (**C**learing **H**ouse **A**utomated **P**ayment **S**ystem)
United States	Fedwire
Uganda	UNIS (**U**ganda **N**ational **I**nterbank **S**ettlement)
Zambia	ZIPSS-Zambian Inter-bank Payment and Settlement System
Zimbabwe	ZETSS-Zimbabwe Electronic Transfer and Settlement System
UAE	UAEFTS UAE Funds Transfer System

Source of Information: https://en.wikipedia.org/wiki/Real-time_gross_settlement

World Customs Organization

EGMONT GROUP
OF FINANCIAL INTELLIGENCE UNITS