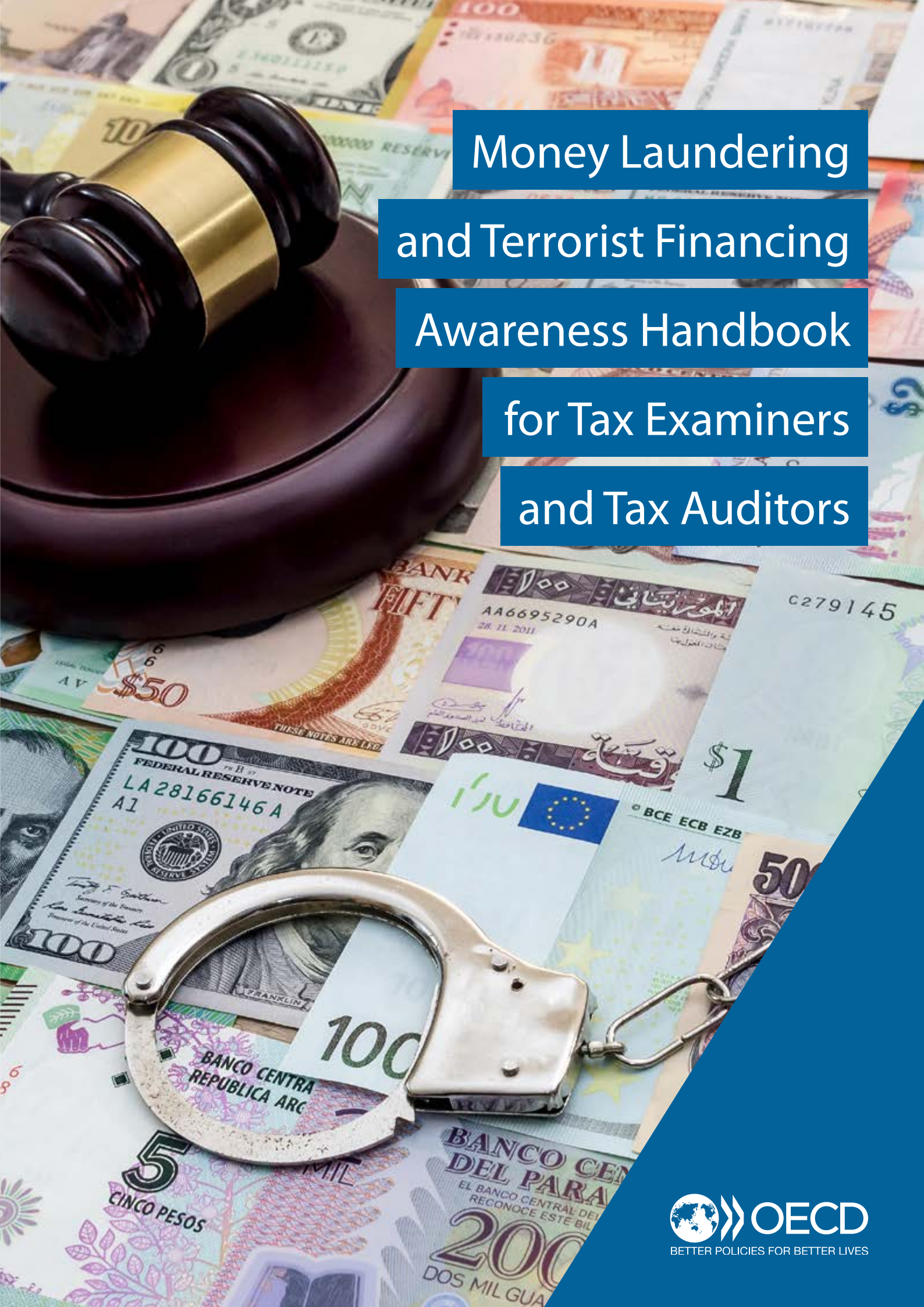


Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors

OECD
BETTER POLICIES FOR BETTER LIVES

Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors

This document, as well as any data and any map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

This document was approved by the Committee on Fiscal Affairs on 10 June 2019 and prepared for publication by the OECD Secretariat.

Please cite this publication as:
OECD (2019), *Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors*, OECD, Paris.
www.oecd.org/tax/crime/money-laundering-and-terrorist-financing-awareness-handbook-for-tax-examiners-and-tax-auditors.pdf.

Photo credits: Cover © RomanR /Shutterstock.com.

Foreword

The purpose of the *Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors* is to raise the awareness level of tax examiners and tax auditors regarding money laundering and terrorist financing. As such, the primary audience for this Handbook are tax examiners and tax auditors who may come across indicators of unusual or suspicious transactions or activities in the normal course of tax reviews or audits and report to an appropriate authority. While this Handbook is not intended to detail criminal investigation methods, it does describe the nature and context of money laundering and terrorist financing activities, so that tax examiners and tax auditors, and by extension tax administrations, are able to better understand how their contributions can assist in the fight against serious crimes.

This Handbook is an update of OECD's 2009 *Money Laundering Awareness Handbook for Tax Examiners and Tax Auditors*. This update enhances the 2009 publication with additional chapters such as "Indicators on Charities and Foreign Legal Entities" and "Indicators on Cryptocurrencies" relating to money laundering. In a separate chapter, the increasing threat of terrorism is addressed by including indicators of terrorist financing.

While the aim of this Handbook is to raise the awareness of the tax examiners and tax auditors about the possible implications of transactions or activities related to money laundering and terrorist financing, this Handbook is not meant to replace domestic policies or procedures. Tax examiners and tax auditors will need to carry out their duties in accordance with the policies and procedures in force in their country.

Table of Contents

FIGURES

Abbreviations and Acronyms

AML	Anti-Money Laundering
ATM	Automated Teller Machine
EC	European Commission
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
GPS	Global Positioning System
GST	Goods and Services Tax
KYC	Know-Your-Customers
LLC	Limited Liability Company
MSB	Money Service Business
OECD	Organisation for Economic Co-operation and Development
PGP	Pretty Good Privacy
REACH	Registration, Evaluation, Authorisation and Restriction of Chemicals
UN	United Nations
VAT	Value Added Tax

Executive Summary

Financial crimes, including tax crimes, money laundering, and terrorist financing, undermine jurisdictions' political and economic interests and pose a serious threat to national security. Law enforcement authorities working to combat these crimes operate in an environment with limited resources, and advances in technology mean that criminals are using ever more sophisticated methods to avoid detection. Combatting these crimes therefore necessitates a "whole of government approach" where different financial crime authorities can pool their knowledge and skills to collectively prevent, detect, and enforce these crimes.

By their very nature, tax crimes are closely linked to other financial crimes and it is well recognised that tax authorities have a central role to play in identifying and reporting money laundering and terrorist financing. While the benefits of reporting and information sharing between tax authorities and anti-money laundering authorities are well recognised, both developed and developing jurisdictions alike face ongoing challenges when it comes to applying this cross-government co-operation in practice.

The OECD originally developed this Handbook in 2009 as a practical tool to enhance co-operation between tax authorities and anti-money laundering authorities. This revised Handbook updates the 2009 version with respect to money laundering indicators, and includes, for the first time, material to raise the awareness of tax examiners, auditors, and investigators of issues concerning terrorism financing.

There are substantial gains to be made by developing strong legal, institutional, operational, and cultural frameworks for tax authorities to report and share information with authorities responsible for combatting money laundering and terrorist financing. Efforts to frustrate these criminal activities start with a firm commitment from political leaders but ultimately end with government officials implementing these policies on the ground.

Authorities around the globe are encouraged to make use of this Handbook and adapt it to their jurisdiction's particular circumstances, taking into account the varying roles that tax administrations have in terms of reporting unusual or suspicious transactions, receiving suspicious transaction reports, and investigating money laundering and terrorist financing offences. Doing so can strengthen the ability of tax examiners and auditors to identify and report money laundering and terrorist financing, thus enhancing the whole-of-government efforts to detect, deter and prevent these illegal and destructive activities.

Introduction

Fighting crime

Traditionally, the job of fighting crime has focused on solving crimes. However, since the 1990s, crime fighters have also sought to deter criminals by paying more attention to the confiscation of proceeds of crime. With the introduction of unusual or suspicious transaction reporting by the regulated sectors, the flow of illicit money or goods is often investigated even before the underlying criminal offence has been detected.

Why criminals launder money

A person who commits a crime will initially try to prevent their actions from being noticed by the tax administration, police and/or law enforcement authorities. If the person is arrested or taxed on the proceeds of crime, they will try to avoid having the criminal proceeds traced back to their illicit origin and avoid their confiscation.

When criminals want to spend the proceeds of their crime, they face a dilemma: how to spend or invest large sums of money without evidence of a legitimate source of income, which could draw the attention of tax examiners or tax auditors. Alternatively, criminals' ability to spend cash on the purchase and use of high value goods or investments may bring them to the attention of law enforcement authorities.

In order to be able to spend money openly, criminals will seek to ensure there is no direct link between the proceeds of their crime and the actual illegal activities. They may also seek to construct a plausible explanation for an apparent legal origin of the illicit money they possess. In this way, criminals seek to "launder" their proceeds of crime before spending or investing it in the legal economy.

Terrorists need financing

Terrorist organisations vary widely, ranging from large, state-like organisations to small, decentralised groups and self-directed networks. Terrorist attacks have also been committed by individuals who have found inspiration in radicalised environments or through self-radicalisation. These "lone actors" also need to fund their activities and they may present particular challenges in terms of identifying observable indicators.

Lone actor terrorists tend to be divided into two main classes: those who are inspired by radical ideas promoted by terrorist organisations, usually located abroad; and those who are radicalised based on a trigger within the environment in which they live (e.g. anti-government). The lone actor terrorist seeks to take the entire process into his or her own hands, from financing him or herself to undertaking the attack.

Terrorists' financing requirements reflect this diversity, varying greatly between organisations. Financing is required not just to fund specific terrorist operations, but also to meet the broader organisational costs of developing and maintaining a terrorist organisation and to create an enabling environment necessary to sustain its activities.

Those who engage in acts of terror require funds to support those activities. From everyday living expenses such as food and shelter, to travelling, training and equipment, to the acts themselves, funds must be raised. These funds may originate from third parties (financiers and supporters) or from their own assets or income, and from legal or illegal sources. Lone actors may self-fund their activities from legitimate sources (e.g. wages or income, savings, credit cards) or illicit means (e.g. crime, terrorist financiers or operators) or receive financial support from others (e.g. family, friends, public benefits, charities etc.).

The direct costs of mounting individual attacks have been low relative to the damage they may yield. However, maintaining a terrorist network or even a specific cell to provide for recruitment, planning, and procurement between attacks represents a significant drain on resources. Significant infrastructure is required to sustain international terrorist networks and promote their goals over time. Organisations require significant funds to create and maintain an infrastructure of organisational support, to sustain an ideology of terrorism through propaganda, and to finance the ostensibly legitimate activities needed to provide a veil of legitimacy for terrorist organisations.

The Financial Action Task Force

The Financial Action Task Force (FATF) is an inter-governmental body whose purpose is the development and promotion of policies to combat money laundering and terrorist financing and other related threats to the integrity of the international financial system. The FATF has developed a series of Recommendations that are recognised as the international standard for combating money laundering and the financing of terrorism. The FATF (and its regional bodies) is the body that monitors compliance with these standards. Many countries have committed to these standards and developed strong and comprehensive frameworks for anti-money laundering and combatting the financing of terrorism, giving law enforcement and security agencies the tools they need to afford better protection from the ever-evolving threats of money laundering, terrorism and organised crime.

Money Laundering

Definition

The FATF defines money laundering as "the processing of […] criminal proceeds to disguise their illegal origin" in order to legitimise the ill-gotten gains of crime.[1]

Why combat money laundering?

Criminals accumulate significant sums of money by committing crimes such as drug trafficking, human trafficking, theft, investment fraud, extortion, corruption, embezzlement or tax fraud. Money laundering is a serious threat to the legitimate economy and threatens the integrity of financial institutions. It also has adverse effects on economic power in certain sectors or industries. If left unchecked, it will corrupt society as a whole. Fighting money laundering serves several purposes.

Societal importance

Crime causes tangible and intangible damage to third parties, individuals and society as a whole. Money laundering can result in reducing the public's confidence in certain professions such as lawyers, accountants and notaries and confidence in economic sectors such as real estate, hospitality and banks and other financial institutions. Investing the proceeds of crime may also distort competition between businesses and entrepreneurs. Money laundering allows the criminal to start, continue and expand activities in legitimate sectors of the economy. It may create a perception that crime pays and may incentivise people to start a criminal career.

To identify tax crimes & other financial crimes

Unusual transactions can indicate tax crimes and lead to the identification of those involved. However, taxing the income of criminals according to tax rules alone will not stop crime from happening or from being profitable. The detection of unusual transactions may also assist in identifying criminals and illegal activities of theirs involving other financial crimes. Sharing information with law enforcement authorities can lead to the start of a criminal investigation.

To locate and confiscate criminal assets

Identifying unusual transactions can provide insight into the flow of money and the eventual conversion of laundered criminal proceeds into assets such as real estate, vehicles, yachts, bank accounts and virtual assets. This will assist law enforcement authorities in seizing those assets during a criminal investigation.

---

[1] FATF (2019), "Money laundering", www.fatf-gafi.org/faq/moneylaundering/ (accessed 1 January 2019).

Legal context

In the vast majority of countries, there is a legal framework for combating money laundering and it is a separate criminal offence in the penal code. The penal code states which activities in relation to proceeds of crime are forbidden and lists the relevant crimes covered, known as predicate (or designated) offences to money laundering. Predicate offences can be defined as "all offences" named in the penal code or can be limited to "serious criminal offences" or a threshold related to the penalty of imprisonment; or can be defined with the help of a combination of these approaches.

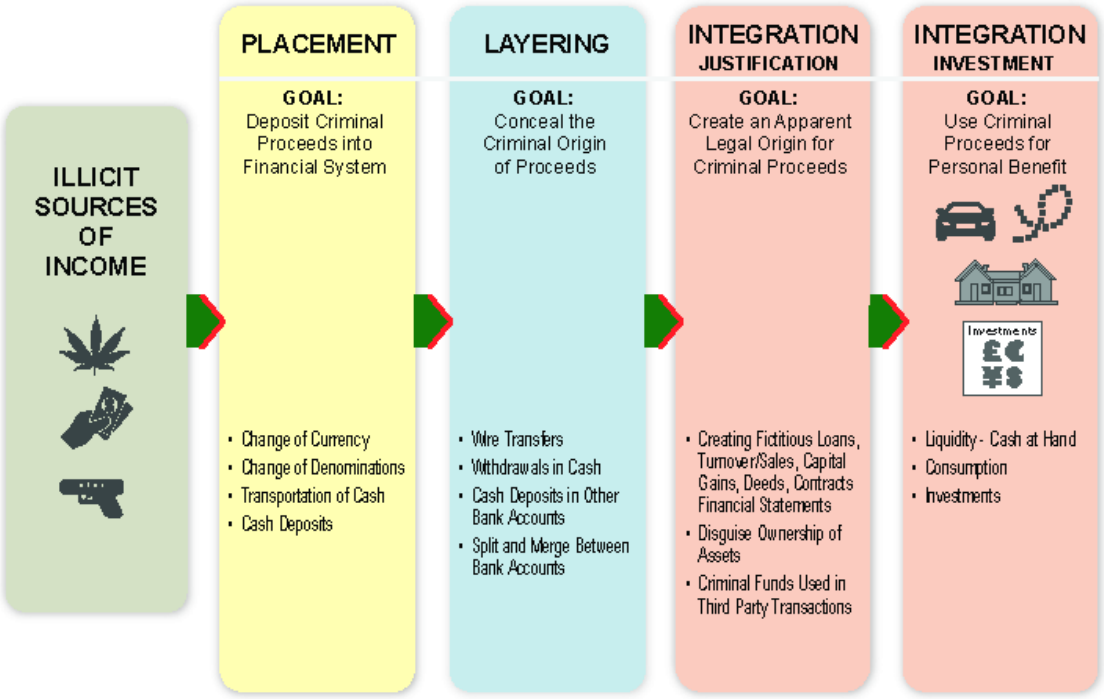
Although FATF Recommendations provide that the legislation should include tax crimes as a predicate offence to money laundering,[2] it is still possible that tax crimes are not included as predicate offences. This means that transactions with money solely derived from a tax crime (e.g. non-reported sales) might not be considered as money laundering offences. However, where the tax administrations in those countries identify indicators of money laundering, it is still of the utmost importance not only to address the serious tax implications, but also to report these transactions to the appropriate authorities in accordance with their domestic legal framework. These indicators could point to proceeds of serious crimes.

The money laundering process

One of the primary needs of tax fraudsters and of those involved in a wide range of criminal activities is to disguise the illicit source of money. This is done by converting the "dirty money" and "washing" it into a form that will be difficult to retrace to its origins. For instance, this could be done by placing the "dirty money" in bank accounts, real estate, stocks, insurance premiums and other assets in the hope that these assets can be used later on without arousing suspicion. Whether the crime is a tax crime, trafficking in narcotics, illegal sales of weapons, corruption or any of a vast range of criminal activities, they all share a basic money laundering process. The process that money launderers use to legitimise the appearance of their illicit proceeds is globally known to take place in three stages: placement, layering and integration. The integration stage may be further divided into two parts: justification and investment. The crime of money laundering is committed at each stage of the process, and it is not necessary for the illicit funds to go through all three stages.

[2] FATF (2012-2018), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, Paris, www.fatf-gafi.org/recommendations.html, Recommendation.

Figure 1. Overview of money laundering



Placement

The goal in this stage is to deposit criminal proceeds, generally cash, into the financial system (usually bank accounts) at home and/or abroad. For this purpose, cash could be switched into other valuables like trade goods, diamonds, gold bars or cheques. Cash can be exchanged into other currencies, in larger denominations and/or split up in smaller sums which allow easy transportation by cash couriers. Cash or other valuables can be transported abroad, away from the country where the crime was committed, to the country of residence of the criminal or a specific country where cash can be easily deposited or invested. Transportation can take place by such means as car, plane, train (passengers or cargo) or boats. Furthermore, cash can be transferred by using an underground banking system. For all of these acts, criminals can use third parties, i.e. either individuals or corporations. Money derived from fraud, such as tax fraud or investment fraud, could also be held in a bank account and therefore, exchanged electronically. Goods from theft can be exchanged for other valuables. Cryptocurrencies are a new asset class for money laundering as they can be transacted anonymously anywhere in the world using the internet. As criminal proceeds no longer solely take the form of cash or money in a bank account, tax examiners and tax auditors should be aware that new and more efficient placement methods may be used.

Layering

The goal in this stage is the concealment of the criminal origin of the proceeds. Money can be transferred and split frequently between bank accounts, countries, individuals and/or corporations, thus distancing it from its criminal origin. Money can also be withdrawn in cash from one location and deposited into bank accounts at a different location. It is common to use bank accounts in countries with strict banking secrecy laws and to nominate offshore corporations as the bank account holders. Cryptocurrencies with an illicit source (e.g. on the dark web) can be sent to a mixing service to conceal the criminal origin.

Integration: justification

The goal in this stage is to create an apparent legal origin for the criminal proceeds. This can be done by:

- Doing business with yourself (e.g. falsifying sources of income, capital gains and/or loans)
- Disguising the ownership of assets
- Using the criminal proceeds in transactions with third parties

The money launderer creates an apparent legal origin of the money by fabricating transactions which are supported by falsified and fabricated documents such as invoices, reports, contracts, agreements, bookkeeping entries, and deeds as well as false statements, both written or spoken. Common justification methods used include:

- Fabricating a loan (e.g. loan-back or back-to-back)
- Fabricating a rise in net worth (e.g. buying and selling real estate and other items, fabricating casino winnings, lottery prizes, inheritance, etc.)
- Disguising the ownership of assets and interest in businesses (e.g. through the use of relatives, foreign legal entities, nominees, etc.)
- Price-manipulating (e.g. over- and under-invoicing)
- Manipulating turnover/sales by commingling illicit and legal sources of income

Integration: investment

The goal in this final stage is to use criminal proceeds for personal benefit. Cash, electronic money and cryptocurrencies can be used for:

- Safekeeping: e.g. cash on hand, cryptocurrencies in a wallet
- Consumption: e.g. day to day expenditures, lavish lifestyle, jewellery, vehicles, yachts, art
- Investing: e.g. bank accounts, real estate, stocks, securities, receivables, funding of legitimate and illicit business activities, repayment of loans

Criminals may want to display their wealth and wealthy lifestyle by acquiring “badges of wealth” such as luxury homes, vehicles, boats, jewellery, etc. Criminals will seek to launder the proceeds from their crimes to pay for these in order to avoid detection by the tax or law enforcement authorities.

Trends in money laundering

The traditional methods of money laundering have centred on the use of cash based businesses and this remains an important area. However, criminals will continue to seek out innovative methods to exploit weaknesses in the financial systems and to try to keep ahead of the investigators. Real estate, loans and trade based money laundering are known methods for criminals to launder the proceeds of crime. These will be described in detail at a later stage.

More recent trends include:

- Cryptocurrencies have, in a relatively short period of time, developed into a new payment method and as a means to store value. Financial transaction systems that are based on blockchain technology promise faster, cheaper and anonymous transactions. The speed and global availability of cryptocurrencies, coupled with the limited regulations, the disaggregation of established financial intermediaries and the potential to hide the true identity of the owners, make them an attractive method for criminals.
- Funnel accounts refer to one or more bank accounts used for illegal funds deposited at one geographical location that gives criminals immediate access to the money via withdrawals in a different geographic location.
- Offshore bank accounts of foreign legal entities continue to be used to make it difficult to track money flows. Overly complex transactions or opaque ownership structures, including sequential or layered legal entities or trusts in multiple jurisdictions, including financial centres, persist. The purpose of these activities is to hide the origin of the funds and their beneficial owners.
- Professional enablers and intermediaries (e.g. attorneys, accountants, trust and company services providers, notaries, estate agents, etc.) traditionally planned and created structures, based on their clients' needs, whether for legitimate or criminal reasons. Their participation usually stops once the entities are formed and accounts opened. Over time, some professional enablers move beyond just establishing money laundering or tax evasion vehicles to actively managing their criminal clients' illicit funds and providing money laundering as a service.
- Third Party Money Laundering Groups form part of an arrangement whereby a criminal organisation makes use of a third party for the laundering of its criminally derived proceeds. The Third Party Money Laundering Group may establish complex and/or durable means of "processing" its clients' illicit funds, without exposure to or knowledge of the clients' predicate offences. The criminal organisation pays a fee or commission but otherwise does not have to deal with the efforts and risk associated with the money laundering activities, allowing it to focus on its criminal activities.

Terrorist Financing

Definition

The FATF defines terrorist financing as the "financing of terrorist acts, and of terrorists and terrorist organisations."[3] It can also involve the facilitation of terrorist acts using other assets or stores of value (such as oil and natural resources, property, legal documents, financial instruments, etc.). The financing can also take place indirectly by storing value in different types of non-financial tangible or intangible assets.

The United Nations provisionally defines terrorism as "[c]riminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes are in any circumstance unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or any other nature that may be invoked to justify them."[4]

Why combat terrorist financing?

Terrorist attacks cause loss of life, serious injury, loss of property and cultivate a climate of fear, undermining the safety and security of citizens. Terrorist attacks have increased in frequency, and can be undertaken on a large or small scale, in collaboration or by individuals acting alone. The spread of terrorist activity can be facilitated by online material aimed at radicalisation and home-grown violent extremism, which has resulted in terror attacks involving improvised explosive devices, firearms, knives, and vehicles.

There has been a significant rise in radical ideas in the political arena of many countries. This represents a threat in regards to their willingness to commit terrorist attacks. Further, extreme nationalistic movements may also represent a possible threat to lives and the stability of democratic nations and processes. These groups contemplating or conducting terrorist acts likewise require funding for their purposes.

Legal context

Most countries have legislation in place combating terrorist financing. Tax examiners and tax auditors should understand how that legislation impacts their work. For example, it may allow or require them to share information with the appropriate authorities when they have a suspicion of terrorist financing or terrorism. It may in some cases even allow them to provide direct support to the investigation. Tax examiners and tax auditors should also be aware of their domestic policies and procedures regarding such legislation and operate within them.

---

[3] FATF (2012-2018), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, www.fatf-gafi.org/recommendations.html, Glossary.

[4] 1994 United Nations Declaration on Measures to Eliminate International Terrorism, annex to UN General Assembly resolution 49/60, "Measures to Eliminate International Terrorism", of December 9, 1994, UN Doc. A/Res/49/60

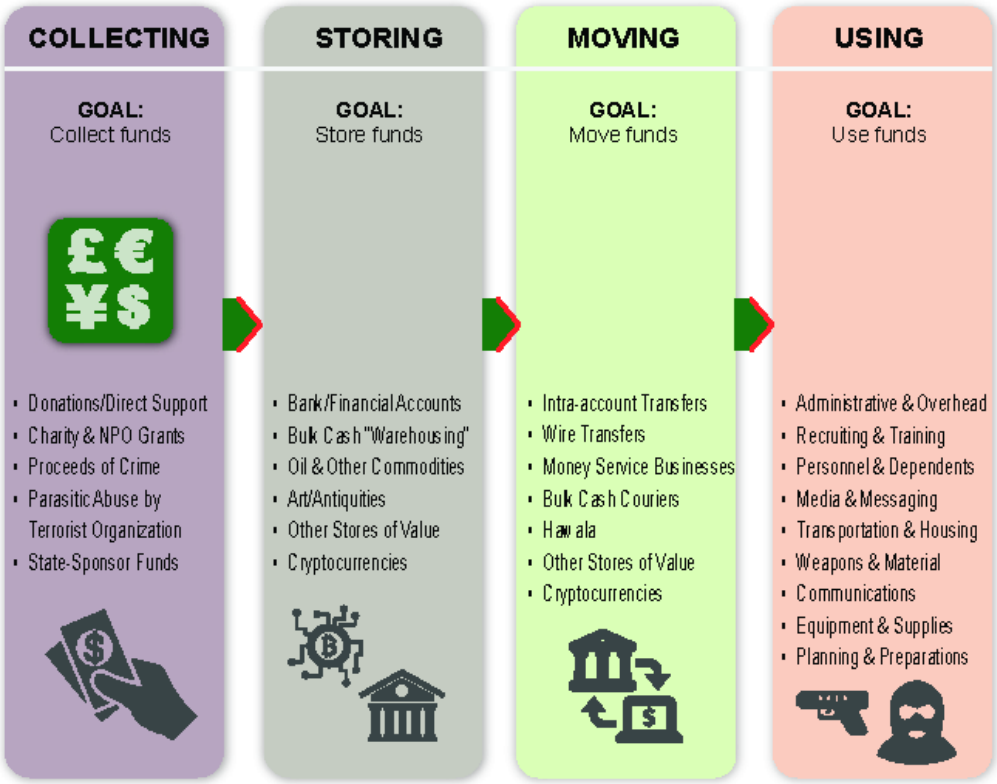
The terrorist financing process

The terrorist financing process involves:

- Collecting the funds intended for use in supporting the terrorist organisation from a variety of sources
- Storing the funds, while determining and planning for their use
- Moving the funds as and when required
- Using the funds as needed to further the terrorist organisation's goals

The terrorist financing model below illustrates these four steps in this process.

Figure 2. Terrorist financing process



Collecting

Typical sources of financial support for terrorist financing include (i) direct donations by individuals and organisations; (ii) use of charities and non-profit organisations; and (iii) criminal activity.

Direct donations: The sources of this financial support are primarily legitimate funds, in amounts large and small, given by individuals, legal entities, non-profit organisations, or businesses, and, in some cases, foreign countries. Such sources include salaries and wages, welfare benefits, personal donations and profits from businesses. Individuals may provide funds from their personal or family's sources of income or support; they may conduct small scale fundraising appeals in their local communities (e.g. neighbourhoods, places of worship, etc.); or broader appeals via the internet, such as on social media and crowdfunding sites. The donors may or may not know the ultimate purpose to which their funds have been applied.

Charities and non-profit organisations: While the vast majority of charities are legitimate and do important work, the FATF has recognised that this sector may be particularly vulnerable to misuse for terrorist financing purposes. Charities and non-profit organisations and similar appeals based on supporting "those in need" are particularly attractive to terrorist financing actors for a number of reasons. They can be successful in obtaining funds from a broad range of potential donors in the public because of the inherent emotional appeal of assisting vulnerable or suffering populations, and many governments encourage giving to charities by allowing taxpayers to deduct the value or a percentage of their donations. If the charities also deal in cash, it is more difficult to trace the funding, movement and use of the funds. Some charities have a global presence and are already working in or have access to other groups located near conflict zones where terrorist organisations may be operating.

Criminal activity: Some terrorist organisations have separate criminal networks to collect funds. Drug trafficking, fraud, cybercrime and white collar crimes are common illicit activities for terrorist financing. For individuals such as foreign fighters and home-grown violent extremists, the abuse of public assistance/benefits programs and the creation of fictitious refunds are identified typologies. Along the way, these criminally-derived proceeds would likely be laundered before they may be directed to terrorist financing purposes. Terrorist organisations occupying large areas may seize the state-owned financial assets and natural resources within the territory under their control. The non-cash assets and resources (e.g. antiquities, crude oil, natural gas, minerals, precious metals and stones) must then be monetised, for example via covert or black market sales, to provide funds for the terrorist organisation's daily use. Those black markets may operate largely outside of the territories or countries where the terrorists are located.

Storing

The storing of funds can be accomplished through means such as:

- Bank and other accounts
- Pre-paid cards
- Bulk cash storage
- High value commodities such as oil, art/antiquities, agricultural products, precious metals and gems, and used vehicles
- Cryptocurrencies

Moving

Well-known mechanisms for moving values include:

- Banking and financial sector
- Remittance sector such as licensed Money Service Business (MSB)
- Informal value transfer systems (e.g. hawala) and foreign exchange houses
- Bulk cash smuggling
- Smuggling high value commodities such as oil, art/antiquities, agricultural products, precious metals and gems, and used vehicles
- Cryptocurrencies

Using

Some examples of the use of funds in terrorism are:

- Terrorist organisations: weapons and material, administrative purposes and overheads, media and messaging, recruitment and training, financial support for personnel and family, communications equipment, transportation, bribing, housing, planning and mission preparation to commit terrorist acts
- Foreign fighters: travel services, passport/visa costs, outdoor/survival equipment, weapons and combat training
- Lone actors and small terrorist cells: weapons and material, vehicles (purchased or rented), minimal financial means to provide for their own food, shelter, communications devices, transport and any procurement requirements for terrorist plots

Some of these uses are day-to-day expenses which are difficult to identify as terrorism related.

Trends in terrorist financing

A significant number of foreign fighters, having been both trained to fight and perhaps further radicalised in conflict zones, survived their combat engagements, exited the battlefield, and returned to their home country. The concern regarding returned foreign fighters is that they will commit acts of terror in their home or neighbouring countries. By referring suspicious behaviour and transactions to the appropriate authority, the tax administration can play a role in reducing the ability of terrorists and their financiers to commit these violent crimes.

Another trend involves the “lone actor” terrorist, which is very difficult to detect. Analysis in the aftermath of attacks has shown that weak signs and small financial traces can be observed. Tax examiners and tax auditors should be aware of this phenomenon and the specific circumstances surrounding it.

The radicalisation process can be very difficult to detect and foresee. Radicalised individuals can be divided in two main groups. First, those known in connection with the radical environment; and second, those inspired by radical ideas promoted by, for example, international terrorist organisations. Only very rarely can indications of this be observed unless there is direct contact with the person who is attempting to conceal their radicalisation.

The lone actor terrorist seeks to take control of the entire process him or herself. The goal of the process is usually to acquire the resources to commit an attack. Where small-scale attacks are chosen as the tactical option, the signs are usually not evident in the data that tax inspectors can analyse and/or audit.

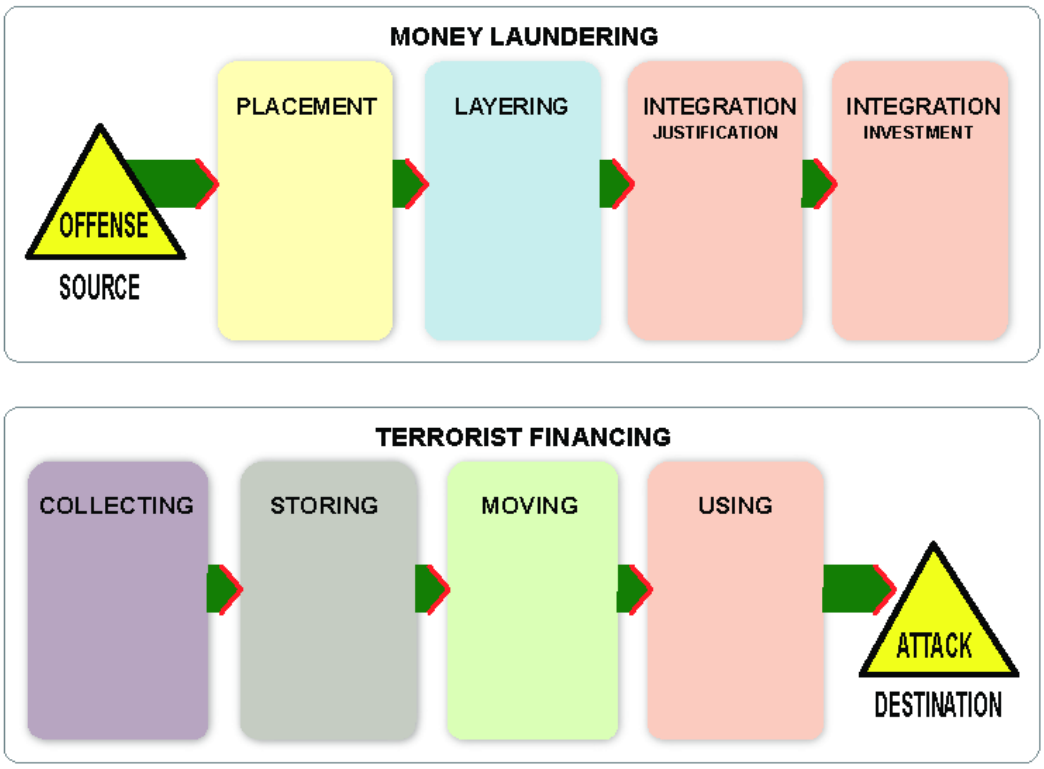
But where the attack has a more complex level and the use of resources is somewhat higher, there are indicators that can be observed.

A lone actor terrorist may use complex efforts, such as tax and VAT fraud, to build up capital in order to lend or provide real estate from where preparations can be made. The fraud will often use a registered company as a front. This company may also be used to acquire goods (e.g. fertilisers or other forms of chemicals or goods that should raise concerns or may even be subject to reporting by retailers). A company or several companies may be used to further cover the movement of goods to the attack site, and to cover or confuse investigators regarding the possible post-attack intentions, and to conceal the involvement of more personnel. By understanding the self-radicalised lone actor terrorist phenomenon, the tax administration can refer the case to the appropriate authorities.

Similarities and differences between money laundering and terrorist financing

The offences of money laundering and terrorist financing may be committed in connection with one another, for example, where funds provided to terrorist organisations are “laundered” funds. Although the activities of money laundering and terrorist financing may share similar attributes and typologies, the timing and direction of their transactions are different. For money laundering, the focus is on the *source* of funds, whereas, for terrorist financing, it is the *use* of funds. Therefore, while secrecy and mobility are attributes sought by both money laundering and terrorist financing schemes, terrorist financing does not usually require a “concealment” or “integration justification” component leading up to the stage at which the funds are used.

Figure 3. Money laundering versus Terrorist financing: Comparing the models



Money laundering is essentially a circular effort: collecting, processing, and returning proceeds of crime "back" to the criminals. While terrorist financing activity is largely a linear progression from the collecting, storing and moving, and onward to the using of funds and assets, whether derived from legitimate or illegal sources.

Self-laundering occurs when the criminal facilitates the money laundering by him or herself. This is also a possible way to observe terrorist financing and the "lone actor". Where the economic funding may be raised at the individual's own initiative (ordinary work, criminality, or other means), the storing may establish a financial basis for the attack; moving to get the money or investments to places where it can be put to use; then used for the attack. The whole process is carried out by the individual.

Accordingly, for the tax examiners and tax auditors, it is important to remember that while there are similarities between money laundering and terrorist financing (e.g. methodologies, mobility, need for secrecy, etc.), the purposes, behaviours and sources of funds are different. The tax examiners and tax auditors need to be aware of the differences so that the appropriate authority can be alerted accordingly.

Role of Tax Examiners and Tax Auditors

Introduction

A country's tax administration is responsible for the assessment and collection of taxes on behalf of the government. This involves gathering and processing information on individuals and corporations subject to tax, including personal details, property ownership, investments, financial transactions and business operations. Tax administrations employ a large number of trained specialists in auditing and analysing financial data and assessing risks. Tax administrations often have extensive powers to access information and documentation from taxpayers and third parties to perform their duties in assessing tax liabilities and preventing, detecting and referring tax crimes.

The role of tax examiners and tax auditors in checking taxpayers' books and records for tax assessments puts them in a unique position to identify not only tax crimes, but also money laundering and terrorist financing. They can help combat money laundering and terrorist financing by identifying and reporting unusual or suspicious transactions in accordance with their domestic law and procedures. The precise models for inter-agency co-operation between tax administrations and anti-money laundering and authorities combatting terrorist financing, and their ability to share information in tax crimes is different in different countries, as noted in the OECD report on Effective Inter-Agency Co-Operation in Fighting Tax Crimes and Other Financial Crimes.[5]

Raising knowledge and awareness

In many countries, tax administrations are partners in the anti-money laundering and anti-terrorist financing regime, as part of the "whole of government approach" in combating financial crimes. Tax examiners and tax auditors are often well placed to identify the first signs of possible money laundering and terrorist financing. Generally their education and training allow them to detect suspicious transactions.

Taking into account that money laundering and terrorist financing are serious offences and given the potential for loss of life balanced against the rights of the individual(s), it is particularly important that tax examiners and tax auditors see a clearer picture regarding a case of potential money laundering, terrorist financing or predicate offences; especially in order to report their suspicion, in accordance with the relevant legislation, to the Financial Intelligence Unit (FIU).

Where a tax examiner or tax auditor refers cases of possible money laundering, predicate offence or terrorist financing to the appropriate authorities (such as a law enforcement authority or public prosecutor), tax examiners and tax auditors should take all the necessary steps to ensure that they comply with the employee safety procedures established by their tax administrations.

---

[5] OECD (2017), Effective Inter-Agency Co-operation in Fighting Tax Crimes and Other Financial Crimes - Third Edition, OECD Publishing, Paris, www.oecd.org/ctp/crime/effective-inter-agency-co-operation-in-fighting-tax-crimes-and-other-financial-crimes.htm.

Critical attitude

Tax examiners and tax auditors must be aware of the need to distinguish between appearance and reality. It is useful to remember the following distinctions:

- Fact: an event or act whose reality has been established
- Assertion: a claim, or an opinion, in the form of a statement or document such as invoices, loan agreements, deeds, tax returns
- Assumption: a presumption or a supposition
- Conclusion: a deduction made based on facts or assertions

Sorting the available information in this manner can assist tax examiners and tax auditors in avoiding conclusions based on assertions or assumptions instead of verified facts. The most important tool for tax examiners and tax auditors is to bring critical thinking to the forefront:

- To evaluate the assertions made
- To question and investigate their own assumptions as a hypothesis
- To draw conclusions based on their knowledge of the techniques used by tax fraudsters, money launderers, terrorists and terrorist financiers

Ultimately, tax examiners and tax auditors should be prepared to inquire further regarding anything that appears to be out of the ordinary, within the context of their required or expected duties. Maintaining a healthy scepticism is critical to assure oneself of the reasons behind anything that appears inconsistent with the usual and expected behaviour.

Tax examiners and tax auditors are reminded that one indicator by itself is usually not a definitive sign that an activity has taken place or will take place. This is of paramount importance when considering possible cases related to terrorist financing. Tax examiners and tax auditors should, when reviewing taxpayer information spanning a year or several years, understand the big picture by considering the many different indicators relating to the various items, e.g. individuals, businesses, as well as cash.

The visibility of unusual transactions

The proceeds of a crime related to money laundering may become apparent to tax examiners or tax auditors. Such visibility is related to, among other things:

- Cash movements as in transporting, exchanging, depositing or spending
- The use of known money laundering methods or processes
- An increase in income, assets, and/or capital gains
- Possessions and/or increased wealth that is not proportionate to the reported income
- Unusual loan arrangements

The funding of terrorism may become apparent also. Such visibility is related to, among other things:

- The collection of funds derived from charities and/or non-profit organisations
- The use of known money laundering methods (movements) or processes (placement)
- Money flows (or other values) to or from conflict zones or neighbouring regions

Detection primarily focuses on unusual transactions that indicate possible money laundering or terrorist financing. “Unusual” means that a transaction differs from the norms of a certain industry or the habits of an individual, taking into account their background, normal activities or declared income. Deviation from the normal or expected behaviour may indicate risk. The greater the deviation in behaviour or the higher the frequency of occurrence of unusual situations, the higher the risk for money laundering or terrorist financing. Subsequently, a more detailed assessment is required.

In general, unusual transactions relating to ***money laundering*** have certain characteristics that make it possible to conceal and justify the illegal origin of the money, the flow of money, the possession of the money or assets derived from it:

- The fact that the origin of the funds is not clear
- The fact that the identities of the involved parties are not clear
- The transaction does not fit the person’s background or reported income
- The fact that there is no economic or logical explanation for a particular transaction

In general, unusual transactions relating to ***terrorist financing*** have certain characteristics that make it possible to conceal and justify the money flows and/or the use of the collected money:

- The collection of funds derived from charities and/or non-profit organisations (e.g. anonymous donations).
- The use of funds for services and/or materials not fitting the profile of the person or organisation
- Money flows (or other values) to or from conflict zones or neighbouring regions under the guise of humanitarian aid

Indicators

To identify unusual transactions, these general characteristics are broken down into the following groups of indicators:

Money laundering indicators

- Indicators for individuals
- Tax return examination and pre-audit indicators
- Indicators for businesses
- Indicators for charities and foreign legal entities
- Indicators for real estate
- Indicators for cash
- Indicators for cryptocurrencies
- Indicators for international trade
- Indicators for loans
- Indicators for professional service providers

Terrorist financing indicators

- Indicators for individuals
- Indicators for businesses
- Indicators for charities and non-profit organisations
- Indicators for cryptocurrencies

It should be noted that an indicator does not provide certainty that an untoward activity has taken place. Genuine and documented explanations for the presence of such indicators may appear during the course of the audit or examination. Not all indicators are equally significant or reliable in predicting or revealing the presence of money laundering or terrorist financing.

It is rare that an isolated, specific indicator can allow the tax examiner or tax auditor to immediately reach the level of reasonable suspicion that there is terrorist financing. This means that additional and substantial indications for terrorist financing (e.g. leads from external, verified sources such as lists available from national authorities, the UN list, etc.) should be observed prior to filing a referral to appropriate authorities.

The reporting of unusual transactions

The reporting of unusual transactions to the FIU by tax examiners or tax auditors will differ within jurisdictions and the requirement to report will be either mandatory or discretionary. All tax examiners and tax auditors should make themselves aware of these requirements so that appropriate action is swiftly taken.

Completing or referring the audit

Tax examiners and tax auditors should adhere to their country's legislation, policies and procedures when considering whether any further audit steps can or should be undertaken if an indication of money laundering and/or terrorist financing is present. If appropriate, the audit should be referred to the relevant law enforcement authority to conduct the criminal investigation on the suspected predicate offence, money laundering and/or terrorist financing.

International exchange of information

Tax examiners and tax auditors should be aware of the international flows of money related to national and international crime. Exchange of information between tax administrations of countries is of great importance in the fight against tax crimes, and may also assist in combatting money laundering and terrorist financing. Where there are legal instruments for exchange of information in place, tax examiners and tax auditors should consider passing on information to another country, in a timely manner, regarding unusual transactions that are relevant for that country, through the competent authority for exchange of information.

Tax examiners and tax auditors should also consider making a request for information from a foreign tax administration if there are issues relating to cross-border activities or transactions.[6]

[6] For more information on the exchange of information between tax authorities, see Global Forum on Transparency and Exchange of Information for Tax Purposes, www.oecd.org/tax/transparency/. The

Role of the tax administration during terrorist post-attack investigations

In addition to identifying risk indicators of terrorist financing and making referrals to the relevant law enforcement authorities, tax administrations can have a role to play in the aftermath of a terrorist attack. The financial information held by tax administrations and their financial investigative and analytical expertise is relevant to a post-attack response. They can provide answers to questions and generate investigative leads to terrorists, financiers and other accomplices.

During a post-attack financial analysis, the flow of money (collecting, storing, moving and using) and participants are important factors to analyse. A review of financial records may establish a financial "pattern of life" and highlight unusual transaction activity or counterparties, which may be further analysed to identify or disqualify individuals and entities as potential co-conspirators or supporters. Transaction records may identify locations where supplies and materials were purchased, providing additional leads for procurement, lodging, and other logistical support.

During this time of stress and elevated tension, the tax examiners and tax auditors are reminded that they should adhere to their country's legislation, policies and procedures, if they are requested to provide such analysis and information.

Global Forum also hosts a secure contact database for tax authorities providing details of the relevant competent authorities for the purpose of addressing such information requests.

Money Laundering Indicators

Indicators for Individuals

Introduction

When performing the audit or examining the tax return there are indicators to consider that will assist in identifying possible cases of money laundering. These indicators may require simple observation skills as well as the examination of the individual's documentation. When individuals spend their criminal proceeds on the acquisition or use of assets and do not have enough legitimate income to explain their expenditures, this is regarded as "unusual possession" or "unusual use" of assets. This in turn raises suspicion. Some criminals will attempt to conceal the origin of the illicit funds by creating an apparently legitimate origin. Passing off the origin of the funds as legitimate can be done by using criminal money to carry out business transactions with oneself or with third parties. The tax examiner and tax auditor should remain mindful that the individual may carry out transactions on their own or with the assistance of a professional service provider.

Indicators

Unusual income

- No income or low income compared to normal cost of living
- Taxpayer appears to be living beyond their means

Unusual rise in net worth

- Inheritance from a criminal family member
- Unexplainable, unexplained or undocumented inheritance
- Voluntary disclosure by known criminals or their relatives
- Unexplainable, unexplained or undocumented gambling and lottery winnings

Unusual possession or use of assets

- A person with low income owns or uses expensive assets (e.g. car, boat, real estate, large amount of cryptocurrency)
- A person owns assets located abroad, usually not declared in their tax return

Unusual debt

- Obtaining a disproportionally high mortgage on a relatively low income
- Obtaining a loan from unidentified parties

Unusual transactions

- Records or reports provided by (or available from) the FIU
- Buying high value assets (e.g. a house) on a relatively low income or without a loan or mortgage
- Buying high value assets far below market value
- Getting a disproportionally high mortgage on a relatively low income
- Taking part in a property flipping transaction with no real estate background
- Cash transaction with an unknown person (e.g. fictitious sale)
- Information from external sources (e.g. law enforcement, media)

Examples

Individual appears to be living beyond their means

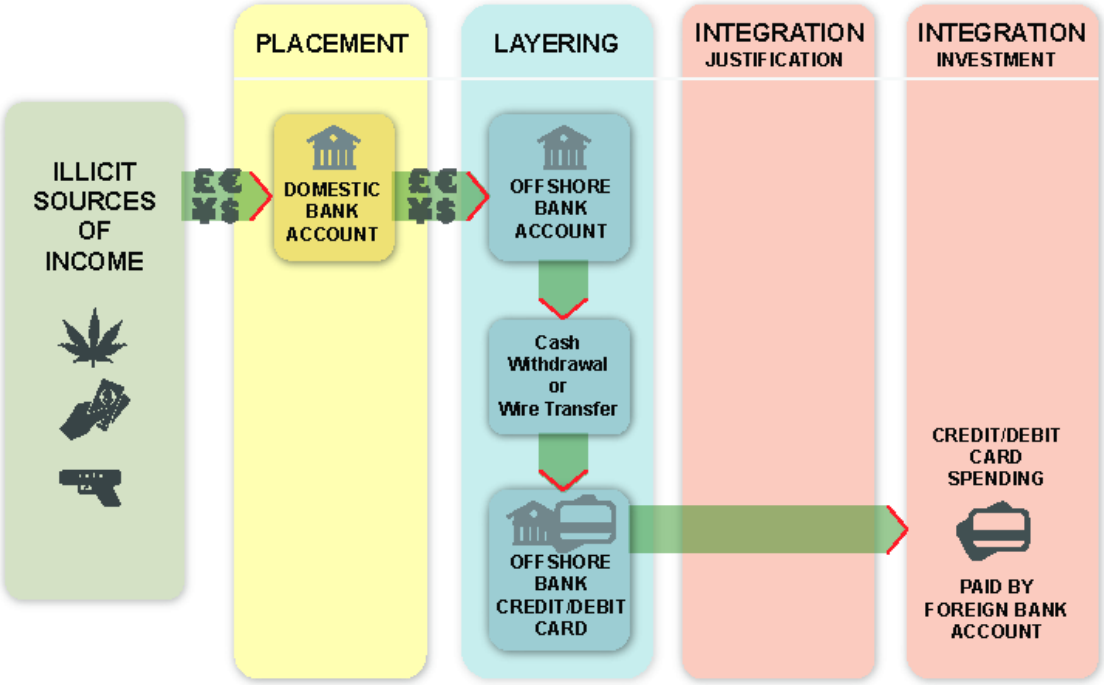
A low family income usually indicates that there are limited opportunities for buying, owning or consuming expensive assets. Therefore, expensive items can potentially be purchased through additional income from crime. The following are examples of such discrepancies:

- A shareholder's financial contributions to a business are not in line with the income reported in the individual's tax returns.
- There is an accumulation of personal wealth when the only known source of funds is from a business source that cannot support it.
- An examination of personal bank records does not show that funds are available to support the lifestyle.
- An individual uses offshore credit/debit cards and the source of funds to support the account cannot be identified.

Debit/credit cards

In this example (Figure 4), the illegal proceeds are deposited into a domestic bank account. These funds are then transferred to an offshore bank account where the money can be withdrawn and used to fund a further offshore bank account which may be linked to a credit or debit card. The foreign credit card can be used at any automated teller machine, point sale, or for online purchases or to make use of the criminal proceeds.

Figure 4. Foreign debit/credit cards



Tax Return Examination and Pre-Audit Indicators

Introduction

This chapter reviews the main indicators in the context of planning for the audit as there are many questions that cannot be answered until the tax examiner or tax auditor actually begins the audit. There is potential for tax examiners or tax auditors to identify money laundering and/or terrorist financing indicators at the start of the audit process. These indicators might be built into the initial checks that are carried out to confirm the scope of the audit and the issues to be audited. Some of these preliminary indicators can relate to tax crimes as well as to other criminal activities. When carrying out an audit of a business, the tax examiner or tax auditor may also audit the individual tax affairs of the business owners. Money linked to tax crimes (e.g. previously unrecorded sales) or other crimes may become visible at some time, for instance through a personal loan to the company or detected in an unreported personal capital gain on the disposal of an asset acquired with questionable funds by the owner of the company.

Indicators

Unusual off-balance sheet items

- Non-transparent ownership of an entity or arrangement
- Ownership of an entity or arrangement by relations/partners of criminals
- International structure with no apparent commercial, legal or tax benefits
- Purchase or sale of a company's shares at a price far above or below estimated value
- Companies/directors registered at a foreign company service provider's address
- Adverse open source information
- Information from closed sources (e.g. FIU, Police)

Unusual balance sheet items

- Ownership contributions of capital are not supported by previous tax returns
- Interest accumulating on loans receivable or loans payable
- Large cash holdings which are excessive for the business

Unusual profit and loss items

- High rise in turnover/sales in comparison to costs of sale
- High rise in profit margin
- Business ratio of costs and sales not in line with industry

Example

Criminals also invest their money in legitimate corporations. They may be interested in a legitimate corporation to earn a return on their criminal proceeds, or because they want to decrease their exposure to risk from their other activities. A legitimate corporation can also be used for criminal activities and criminals can attempt to launder money in the buying, financing and running of legitimate companies. An indicator is the buying of shares at a price way below estimated value or net worth of the company. The balance of the true price may be paid “under the table”. Another indicator is a relatively high capital gain compared to the length of time the company was owned. This may indicate the use of criminal proceeds at the time of purchase. In this situation a simulated capital gain is bought by asking the buyer to pay an inflated price while refunding the inflated portion of the price to the buyer with the proceeds of crime.

Indicators for Business

Introduction

In the course of conducting the pre-audit review and developing the audit plan, it is not uncommon to identify unusual indicators, which should be examined during the audit. Even the creation of a business itself could be an indicator. During the audit, the examination of individual transactions may disclose tax risks as well as money laundering indicators.

Indicators

Unusual transactions and parties

- Entrepreneur demonstrates poor knowledge of the business
- Transactions in goods or services do not fit company's profile
- Transactions without an evident commercial basis
- Transactions or agreements without relevant supporting documents
- Transactions with offshore companies
- Transactions with suspected criminals or their partners
- Non-transparent/non-identifiable customers, creditors or lenders
- Transactions with business associates or customers that share a common address
- Transactions identified as asset sales but assets cannot be substantiated

Unusual money flows

- Payments to or from third parties who are not involved in the transactions
- Payments to or from unrelated offshore companies or accounts
- Company bank account used as a cash flow-through account
- Non-transparent or non-verifiable origin of the money (e.g. cash deposits, loans or sales)
- Denominations and currency not the norm in the industry
- Bank deposits not declared as turnover/sales
- Money flows without apparent economic reason or supporting documentation
- Unusual use of credit cards or debt instruments
- Profit sharing agreements with no relevant economic basis

- Lack of relevant supporting documentation
- Costs incurred not leading to turnover/sales

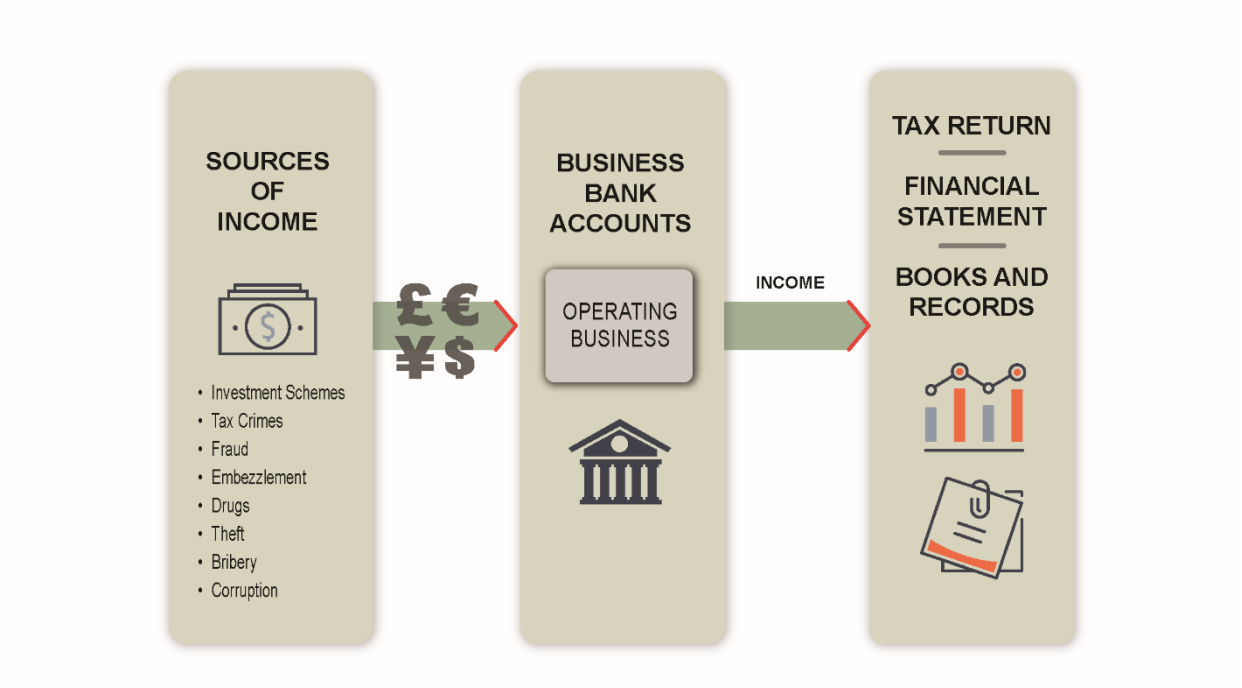
Unusual turnover/sales

- Significant increase in (anonymous) cash turnover/sales
- Large cash payments received for luxury goods sold
- Large cash payments received for goods never delivered (fictitious buyer)
- Transactions without an evident commercial basis or supporting documentation on file
- Transactions and agreements without related costs or relevant supporting documentation
- Transactions with suspected criminals or their partners
- Transactions in goods or services do not fit company's profile
- General description on invoices relating to high-cost items
- Cost of sales invoiced by non-transparent corporations
- Profit sharing agreements with no relevant economic basis
- Lack of relevant supporting documentation
- Costs incurred not leading to turnover/sales
- Transactions with (known) fraudulent parties (e.g. missing traders)

Examples

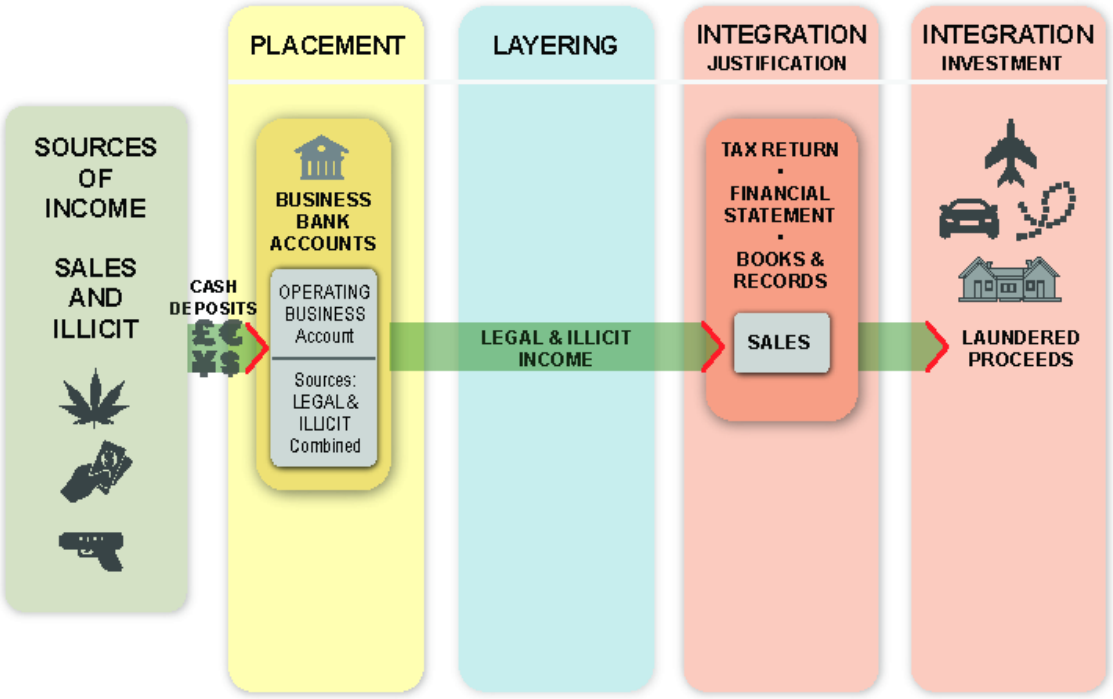
Significant increase in (anonymous) cash turnover/sales

Figure 5. The business at first glance



In this scheme the proceeds of crime are recorded as sales. Because the proceeds of crime are mostly cash, in many cases cash sales are fabricated so that clients and the origin of the money cannot be identified. Tax examiners and tax auditors should remain aware that a superficial examination of the information and records available may appear very straightforward and may not raise suspicion that money is being laundered.

Figure 6. Fabricated sales



What is actually happening is that the criminal is depositing the illicit funds into the business bank account along with funds from genuine sales. The illicit funds are recorded in the books and records as if the money came from genuine turnover and the overstated income is reported in their tax returns. The company may not always have to pay corporate tax on this increased income if the company has trading losses available or where false deductions or a higher salary for the director (i.e. the criminal) are also created.

Indicators for Charities and Foreign Legal Entities

Introduction

Charities and non-profit organisation sectors have been vulnerable to being used wittingly or unwittingly, to receive and disburse funds in support of criminal activities, including money laundering. Although the vast majority of charities and non-profit organisations conduct worthy and critically needed philanthropic work around the world, tax examiners and tax auditors should be aware that these sectors are at risk.

Governments encourage charitable giving by allowing donations to certain categories of organisations to be tax deductible, thereby allowing individuals and businesses to reduce their taxable income. Donations must be made to a designated tax-exempt entity such as a registered charity or non-profit organisation in accordance with a country's relevant legislation in order to trigger such a tax deduction.

Foreign legal entities and arrangements, such as foundations, trusts, shell companies, and special-purpose vehicles, remain an important means by which criminals may attempt to hide assets or to evade the scrutiny of the authorities in their financial transactions. This includes hiding the origin or destination of the funds and the beneficial owner of assets.

Indicators for charities and non-profit organisations

Unusual transactions and parties

- The entity is not registered/documented with the competent authority or jurisdiction
- The entity has little or no physical or online presence
- Unusually high amount of cash deposits or withdrawals
- Cash deposits in large denominations
- Transfer of funds or other assets to unrelated accounts or entities
- Spending funds for other than stated purposes
- Principals, directors, officers, or key employees of an entity showing unusual rise in net worth
- Principals, directors, officers, or key employees of an entity are subject to negative open source information
- Lack of transparency, direction and control in fundraising or expenditures

Indicators for foreign legal entities

Unusual transactions and parties

- Use of overly complex transactions when a conventional method is available
- Entity managed by a Trust and Company Service Provider
- Transactions without an evident commercial basis
- Transactions or agreements without relevant supporting documents
- Corporate structure includes multiple companies or jurisdictions without economic or fiscal reasons
- Transactions with suspected criminals or their partners
- Being evasive or reluctant to provide beneficial ownership information
- Beneficial ownership cannot be determined
- A person with effective control of the foreign entity or its assets is different from the official nominee director

Unusual money flows

- Payments between the foreign legal entity and a domestic party without supporting documents
- Domestic bank account being used as a cash flow-through account
- Non-transparent or non-verifiable origin of the money
- Investment made by a foreign legal entity for the benefit of a domestic individual, e.g. apartment, yacht

Examples

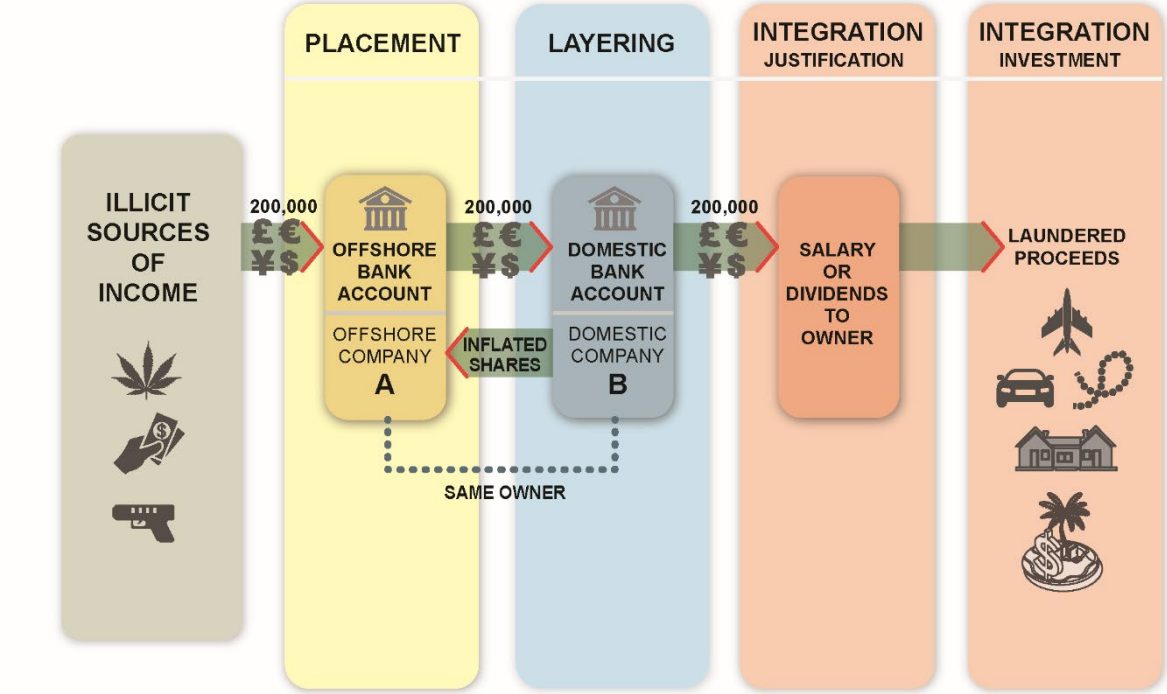
- An offshore company is behaving “un-businesslike” or is acting in violation of current or common economic experience rules, for instance in cases where funds are channelled out of a country using money remitters and offshore trusts.
- An offshore company can own assets domestically. The use of these goods by persons with a criminal background or insufficient income could point to a money laundering scheme.
- Fictitious declarations for Value Added Tax (VAT) refunds play an important role in the concealment, shifting and investment of criminal proceeds as well as in the concealment of the true beneficial owners. An offshore corporation can be quickly established and managed by a local company service provider also acting as a nominee director, often located in a strict bank secrecy jurisdiction with no obligations for publication of annual accounts.

Non-transparent ownership

When shareholder relationships are transparent, the true beneficial owner is visible. This beneficial owner will also declare their shares and any income earned from the business on their income tax return. If transparency is absent, the identity of the true beneficial owner is hidden. Criminals conceal the assets of criminal origin in this way so they can continue to use or enjoy the assets or obtain a return on their illegal money. The lack of transparency in a shareholder relationship is an indicator for the concealment of assets with a criminal origin.

An important tool for the concealment of the true beneficial owner is the use of offshore entities, such as offshore corporations or trusts. An offshore corporation is a legal entity incorporated in a foreign jurisdiction and usually only conducts economic activities outside the country in which it was incorporated. Such companies play an important role in the concealment, shifting and investment of criminal proceeds as well as in the concealment of the true beneficial owners. An offshore corporation can be quickly established and managed by a local company service provider also acting as a nominee director, often located in a strict bank secrecy jurisdiction and with no obligations for publication of annual accounts. This case illustrates the techniques used:

Figure 7. Non-transparent ownership



In the case illustrated, the criminal wants to launder USD 200 000 of illicit income. These funds are deposited in an offshore bank account controlled by offshore Company A which is owned by the criminal. The criminal wants to have these funds available to them in their home country. The funds are subsequently wired to a domestic bank account by Company A for the purchase of shares in Company B which is also owned by the criminal. An inflated value of an additional USD 200 000 is placed on the shares of Company B. Company B now has USD 200 000 in its account available to the criminal. These funds are now laundered and can be integrated as seen in Figure 7.

Indicators for Real Estate

Introduction

Real estate has long been a preferred choice of criminals for hiding illicit funds, and manipulating property prices is a typical means to transfer proceeds illegally between parties. There are other factors that also make real estate appealing: the relatively high monetary value, the likelihood that the value will appreciate over time and the opportunities to conceal ownership. The following techniques are identified:

Purchasing: in purchasing a property the criminal will seek to launder proceeds by providing a portion of the purchase price (from criminal proceeds) in cash or other values “under the table”, with the formal sale documents showing the balance of the purchasing price. The purchase of real estate by offshore companies, where the shareholder and the origin of the money is concealed, is also a way of using criminal proceeds.

Financing: a popular form of money laundering is by financing through loan back. This is when a criminal borrows their own criminal money. This is simply done by creating a loan agreement between the criminal or their representative and an apparent third party. Foreign offshore corporations controlled by the criminal are most commonly used as the third party lender.

Renovating of real estate: the owner of the property has it altered and pays for renovations with criminal money.

Selling: selling real estate property to an offshore corporation, for a price that is much higher than the real market price, creates a seemingly legitimate capital gain. Selling real estate property to a third party for a price above market value, while giving a cash rebate at the same time, will also create a seemingly legitimate capital gain.

Concealment of ownership: the criminal will attempt to conceal their assets, wealth or the origin of the funds used to finance the purchase. Examples include:

- Straw man/straw men or nominees, perhaps a relative of the criminal or a corporation, often offshore, is used as the registered owner of the real estate property. The criminal is therefore able to remain anonymous.
- Third party bank accounts or trust accounts, administered by notaries or lawyers, are used to conceal the origin of money to acquire the property.

Use of real estate: luxury homes can be rented and the lease can be in the name of a third party, and used by the criminal. The rent is paid in cash, out of criminal proceeds.

Indicators

Unusual parties

- A non-professional party involved is a-typical (very large, specialised and/or with high risks)
- The party belongs to the social network of a criminal
- There is non-transparency in the ownership of a legal entity

Unusual possession

- Non-transparent ownership (e.g. bearer shares, legal entity not known by the tax administration)
- Lack of income in relation to purchase price
- Persons with criminal records or background
- Social network of a criminal person
- Fast growing portfolio

Unusual transactions

- Unusual transaction prices (e.g. out of line compared to prior transaction price, asking price or market value)
- Unusual transaction results (high profit during a short period of ownership)

Unusual financing

- Unusual origin of the funds
- Unusual lender
- Unusual borrower
- Unusual loan agreement
- Unusual financing results

Unusual occupant or user

- Lack of income in relation to fair market level of rent
- Persons (or those related to persons) with criminal records or background

Unusual statements given

- Highly unlikely, non-verifiable or non-documented statements given

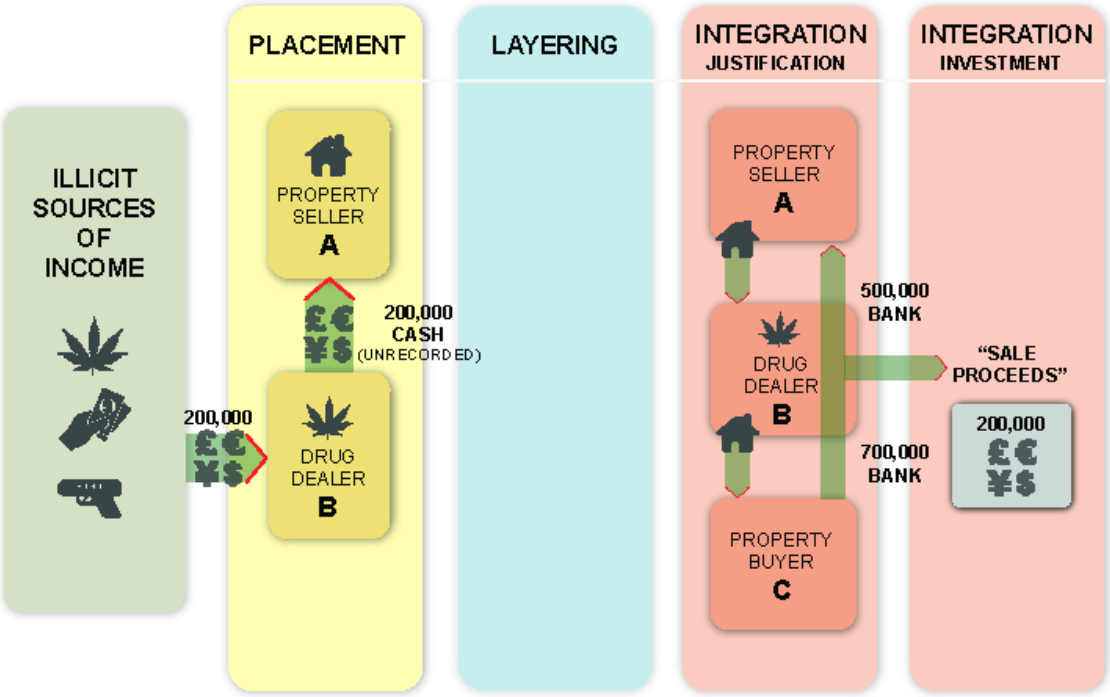
Example

Property flipping

Property flipping means that two or more transactions relating to the same property take place within a relatively short period of time. Property flipping can be used to launder criminal proceeds. The buyer pays more than the price which is documented in the purchase agreement and the notarial deed. When the buyer subsequently resells the property for the same price that they actually paid, it appears that they have made a profit. As a result of this transaction, the criminal proceeds have been converted to a seemingly legitimate amount of deposit money.

In this example, the criminal seeks to launder USD 200 000 with the apparent legitimate purchase and subsequent sale of a property. The property seller receives full market value (e.g. USD 700 000) for the property, but agrees to receive an “under-the-table” cash payment of USD 200 000 and a formal payment of USD 500 000 along with notarial documents listing the sale as USD 500 000. When the buyer subsequently resells the property for the same price that they actually paid (USD 700 000), it appears that they have made a profit.

Figure 8. Property flipping



Indicators for Cash

Introduction

It is common knowledge that drug trafficking generates large amounts of cash in small denominations and, depending on the country where the sales are made, in certain currencies. The proceeds of other types of crime like theft, investment fraud and tax fraud can also generate large amounts of cash. Payments between criminals will be largely in cash. As a result, the criminal is left with the problem of having to clean all this dirty money. Consequently, focusing on the cash can lead to the detection of criminals, their proceeds, their criminal activities and their money laundering activities.

The possession of cash has advantages for the criminal, namely its anonymity regarding origin, possession and use. For criminals, the anonymity of the origin gives them the opportunity to create the appearance that the money was derived from an apparently legitimate source. For example, fictitious loans can be set up or illicit funds can be comingled with legitimate sales receipts where taxes may even be paid. Furthermore, possession of cash and its use does not usually leave a connecting paper trail and the owner's identity is often not recorded.

Cash also has disadvantages. It is common knowledge that the possession and the use of large sums of cash or its possession and the use of large denominations of a currency can point to proceeds of crime. Also, the particular currency used could point to a specific country of origin where the bearer of the money does not have any economic presence. Along with the practical problems associated with physically moving large amounts of cash, a significant problem with regard to cash is its limited spending and investing possibilities. Due to the risk of counterfeit, theft and the high cost of handling cash, businesses are not willing to accept large payments in cash. Also, anti-money laundering (AML) regulations, where the identification and reporting of transactions is required, make it risky for the criminal to spend the money carelessly.

Indicators

Unusual origin of the funds

- Cash received from countries with a high level of corruption or political instability
- Countries with a well-developed financial system (as a safe and cheap alternative to cash transports)
- Cash deposits into business and personal bank accounts from unexplained sources

Unusual explanations given

- Incomplete, unlikely, partly incorrect or no explanation given for the origin of the cash
- No correspondence or supporting documentation in relation to the origin or owner

Unusual possession

- Amount, denomination, or currency do not fit the bearers' personal or business background

Unusual method of transportation

- Concealed transportation of cash
- Clear safety risk in method of transportation
- High costs of transportation compared to alternative methods of transport

Unusual destination and spending

- Countries of risk (e.g. drug producing, ineffective AML regulation, strict banking secrecy)
- Cash received in countries which do not fit bearers' background
- Cash spent on luxury items
- Large cash withdrawals or payments without an economic reason or explanation

Unusual cash flows

- Cash turnover/sales not to be expected in industry
- Large increase in cash turnover/sales from non-identifiable customers
- Deposits or drafts in cash in denominations or currency not to be expected in the industry
- Cash deposits which are not registered as turnover/sales
- Foreign loans received in cash and in local currency
- High cash investment by foreign owner of lender
- An occasional high cash transaction (e.g. turnover/sales, cost invoice)
- Structuring of bank deposits: smaller transactions in a short period of time, to avoid reporting (smurfing)

Examples

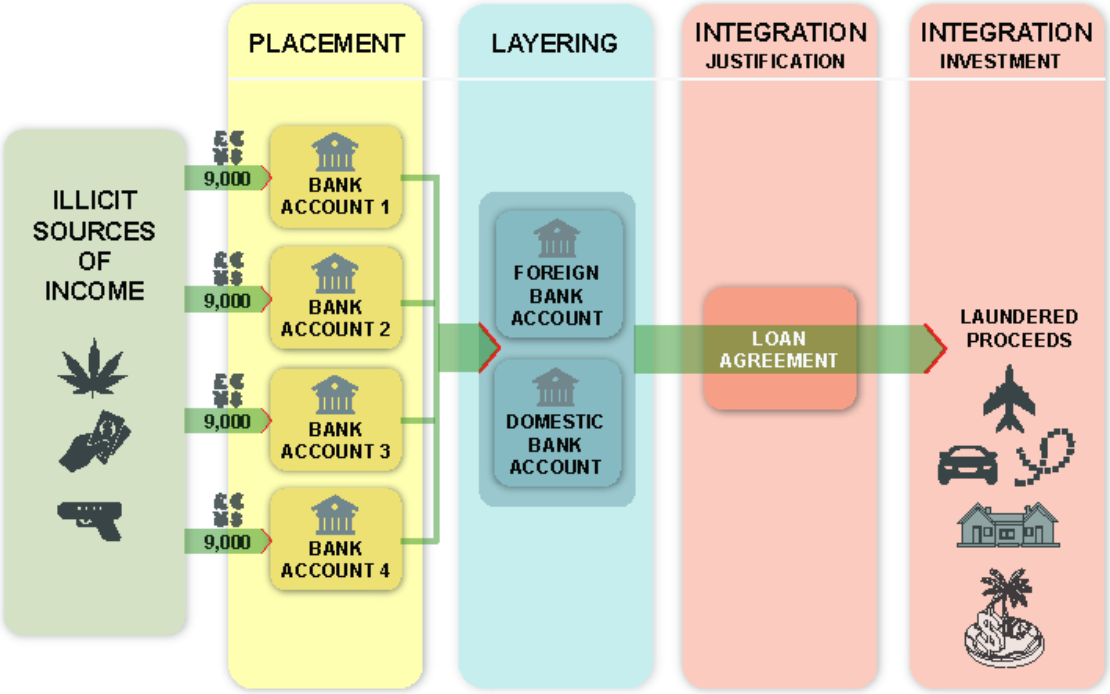
The laundering of cash can consist of:

- Converting the cash into other denominations or currencies using exchange offices, banks, the black market and through the use of cash driven businesses
- Physical movement and transportation by car or plane using couriers
- Depositing money in the banking system through the use of "straw men" (nominees), the use of cash driven businesses or the use of the "smurfing" technique
- Creating an appearance of a legitimate origin by creating fictitious loans or fabricating cash turnover
- Making cash purchases

Example: smurfing

In the example which follows, illicit funds are "smurfed" into domestic bank accounts in amounts below the threshold where the banks would be required to file a currency transaction report or make a report of an unusual or suspicious transaction. From there the money is transferred to foreign and domestic bank accounts where the funds are used to make a "loan" to the criminal. All these acts can be committed by the criminal or by a third party, domestically and/or abroad.

Figure 9. Structuring "smurfing"



Example: countries of risk

Certain countries are considered to be attractive to criminals for their criminal activities and/or money laundering purposes. Governments may prepare a list of such countries that present high risk features. For example, this may include countries that are known for the production and exportation of illegal drugs, whereby cash will flow back to the criminal organisations in the drug-producing countries. A list may also include countries where effective anti-money laundering controls are not yet in place and which a criminal may consider attractive for depositing money as well as countries geographically close to the illegal activity, with strict banking secrecy laws and a lack of transparency associated with beneficial ownership.

Having a bank account in such a risk country may indicate money laundering. Cash in small denominations or cash in currencies of countries where individuals or corporations do not have registered legal activities can indicate that the proceeds are from the sale of drugs. The amount of cash, the denominations and currencies can lead to problems with transportation, issues relating to an apparent legal origin or for spending the money. For these reasons, illicit money will be exchanged into larger denominations and/or into another currency. Normally such a transaction may be identified as suspicious by the customs agent

or the bank receiving the deposit, but tax examiners or tax auditors may also detect money laundering here by identifying a pattern of transactions over a period of time.

The following example is based on a real case. A person is travelling from a country in Central America, the country of risk, to Paris declaring EUR 125 000 in notes of EUR 500. The story the traveller told is that the amount was from legitimate foreign exchange activities in the Central American country. He said that he was transporting cash in Euros from the Central American country to Europe; he deposits the money into his bank account in Europe, flies back to Central America and withdraws the cash from ATM (automated teller machine) in the local currency. The local currency is then exchanged on the local black market for Euros at a profitable rate. Once again, the individual flies back to Europe and deposits the money into his bank account. All the while, cash is being declared at customs, profits are being declared and taxes are paid.

From a fiscal point of view, while there are no issues but the excessive amount of currency exchanged and physically transported, the large denominations and the Central American country of origin should raise suspicion. As it transpired, the real story is that this person was helping a large drug organisation in Central America to change their proceeds, paid in Euros, into local currency to make payments possible (e.g. production, transport, security, investing) in Central America.

Indicators for Cryptocurrencies

Introduction

A cryptocurrency is a form of "virtual asset," as defined by the FATF. Cryptocurrencies are fully based on cryptography; both in the creation ("mining") of this type of asset, the storing of value, as well as in terms of the security of the payment system. With the increased use and possession of cryptocurrencies, it is important for regulators and law enforcement agencies to understand, monitor and protect against the risks posed by such assets. Cryptocurrencies enable users to directly transfer value to one another without using a third-party intermediary, bypassing the bank system. Bitcoin, which is a decentralised payment system with its own virtual coin, was the first full cryptocurrency based on a new technology, the blockchain.

In recent years, the use of cryptocurrencies has emerged as a new form of storing, or moving, value and making payments, and there are currently thousands of different types of cryptocurrencies. As the technology in this field continues to develop and evolve, so too will the techniques of criminals in committing financial crimes, and the demands upon law enforcement to identify and mitigate these risks will increase. This chapter provides an initial set of descriptions and risk indicators; however, this will be a field where it is important for tax examiners and tax auditors to ensure their knowledge keeps pace with developments.

Transactions and anonymity

Generally, the value of a cryptocurrency is determined by supply and demand at cryptocurrency exchanges, which are a form of virtual asset service providers. An exchange is an online trading platform where cryptocurrencies are traded via a mechanism of supply and demand against other cryptocurrencies or fiat currencies. Transactions are made from and to addresses linked to a digital wallet. This wallet can be managed by the user directly or through a third party, such as an exchange. Transactions are irreversible and can be seen by anyone via the blockchain and certain websites on the internet. There is no identity linked to a wallet address and to individual transactions. The identity of the user may only be known to the wallet provider or the exchange if the user chooses to make use of such providers.

An increasing number of countries' financial authorities are defining and regulating cryptocurrency exchanges as Money Service Businesses (MSB) – subject to the same AML regimes. In the face of continuing global regulatory scrutiny, another form of cryptocurrency exchange has emerged: a peer-to-peer exchange. Unlike the other exchanges, peer-to-peer exchanges connect buyers and sellers of cryptocurrencies and allow them to conduct direct transactions. This provides a means of circumventing the know-your-customers (KYC) protocols which may not apply to the peer-to-peer exchanges, adding another dimension of complexity relating to cryptocurrencies.

Users

Next to the developers of blockchains and the cryptocurrencies, there are the miners of the coins. New coins are algorithms that are extremely difficult to crack. These algorithms are cracked with the help of computing power. These miners not only unlock new coins and add these to the network, they also check transactions in the network. Next to the miners, there is a group of early adopters, who are interested in new technologies. The use of cryptocurrencies is widespread on crypto platforms, among businesses, private persons (e.g. consumers, speculators, investors, traders), and, last but not least, among criminals.

Risks

As cryptocurrencies offer a certain amount of anonymity, they have attracted the interest of tax evaders, fraudsters and other criminals. Criminals for example pay other criminals for illegal goods and services on the online dark-web markets (e.g. drugs, weapons, stolen credit card details and ransomware). Non-face-to-face transactions on the dark-net markets can often only be performed using cryptocurrencies.

Criminals generating their income and wealth using cryptocurrencies may need to convert (part of) these cryptocurrencies into cash, the so-called “cash out.” There are different methods to cash out (cryptocurrency to cash):

- Use of an exchange: a criminal can create an account on an exchange, transfer his or her cryptocurrencies to this exchange, then sell it for fiat currencies and have the exchange transfer the money to their (foreign) bank account. This money can eventually be withdrawn at an ATM. Another option is to use a front person for this process.
- Use of cryptocurrency traders: there are also individual traders who offer to exchange cryptocurrencies (face-to-face) for cash, for a high fee of course.
- Use of cryptocurrency cards: there are also prepaid cryptocurrency cards which allow cash withdrawals at regular ATMs and online payments, including those issued by foreign legal entities.
- Use of coin ATMs: there are also special coin ATMs available which allow the exchange of cryptocurrencies for fiat currencies and vice versa.
- Use of online casinos: online casinos with weak know-your-customers (KYC) protocols accept deposits in cryptocurrencies, which are then transferred into player’s gambling balance. These can instantly be withdrawn to either an onshore or offshore bank account, prepaid credit cards, crypto-currency debit cards and using payment services via Money Services Businesses (MSB).

Next to cashing out, criminals can also use cryptocurrency traders and coin ATMs for buying cryptocurrencies using their illicit proceeds of crime (cash to cryptocurrency). This allows them to buy illicit goods on the dark-web markets or use it as a store of value.

Indicators

Unusual transactions

- Trading or having coins available from mining without relevant equipment or electricity costs to show for
- Accepting, trading or having coins available with a history on the dark web
- Withdrawal of large amounts of cash from the bank account shortly after having received money from cryptocurrency exchanges
- Paying high fees for converting (selling) cryptocurrency in exchange for cash
- Large deposits of cash into personal accounts, followed by purchases of cryptocurrencies from commercial/regulated exchanges
- Use of a debit card fuelled by cryptocurrencies
- Large cash deposits and large cash withdrawals via coin ATMs
- Cryptocurrency transactions for the purchases of luxury items that seem not in line with the buyers reported income
- Unexpected amounts of cryptocurrency in the business (sales or loans)

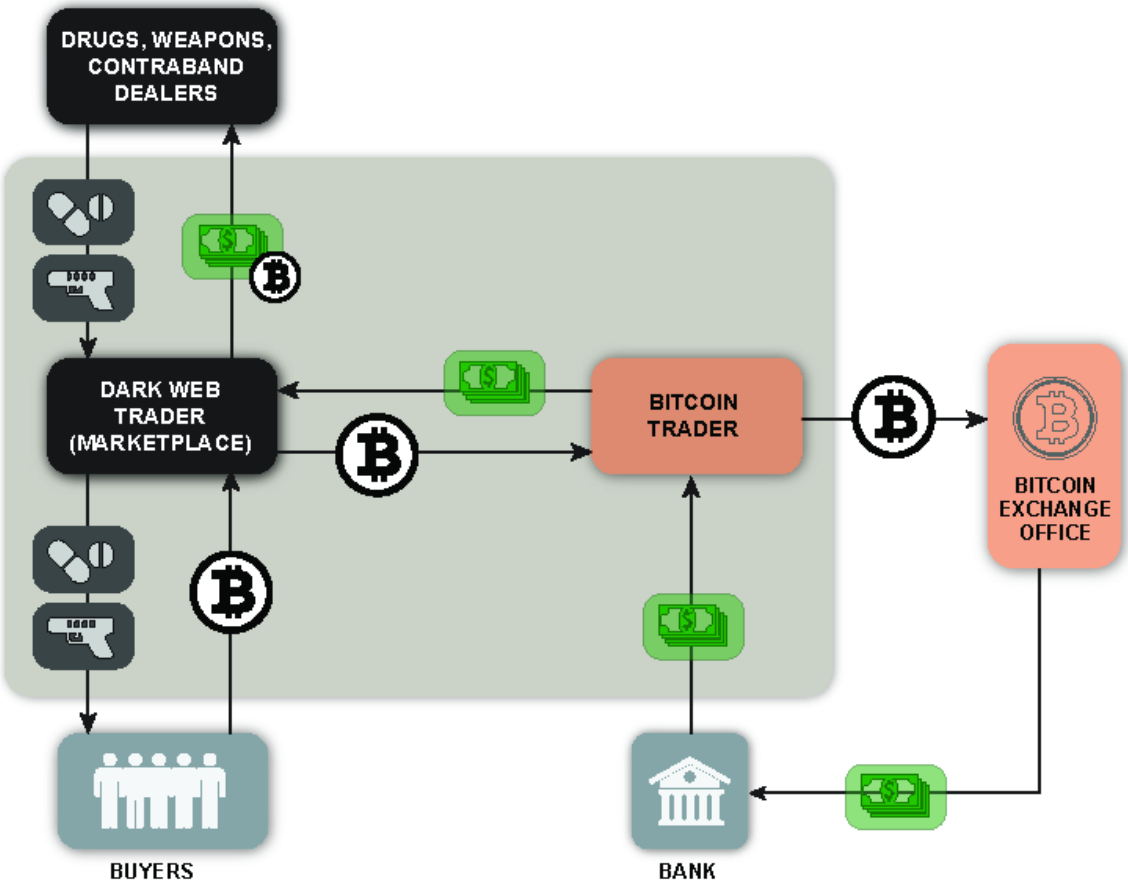
Unusual behaviours

- Unable to justify the economic or business benefit of transactions involving cryptocurrency
- Transactions in cryptocurrencies which have at least two of the following features:
    a) The seller or purchaser offers their services via demand and supply sites on the internet
    b) The parties do not establish each other's identity
    c) The seller or purchaser protects their identity
    d) Cryptocurrencies are paid for in cash
    e) The exchange fee is unusually high
    f) The transaction is conducted in a (public) place where a lot of people are present, which decreases the safety risks for the seller and purchaser
    g) A legal economic explanation for the way the exchange was made is not likely
    h) The scope of the purchased virtual currencies is unlikely in relation to the average private use
    i) The exchanger is unknown to the Chamber of Commerce and the Tax Administration
- The purchaser and/or seller make(s) use of a so-called mixer or tumbler

Example

A schematic representation of a criminal cash flow via the Bitcoin trader.

Figure 10. Bitcoin trading: illicit goods



The trader of illicit goods, whose identity is hidden on the dark web, is selling illicit goods in return for cryptocurrencies. The criminal wants to convert his available cryptocurrency into cash and for this purpose he contacts a local Bitcoin trader. In a face-to- face meeting, Bitcoins are exchanged for fiat currencies. With these fiat currencies, the criminal is able to finance his expenses. The Bitcoin trader sells the Bitcoins to an official exchange and receives fiat currency on his bank account.

Indicators for International Trade

Introduction

In international literature, money laundering through trade is known as “Trade-Based Money Laundering”. It is seen by various organisations, such as the FATF and the World Customs Organization, as one of the key methods to move and/or launder large amounts of money derived from crime. The movement of money can be visible through the payment of expenses. Money can also be visible when it is moved via air transportation, road transportation or when smuggled with goods. It should be noted that while the focus here is on international trade, the same methods may be used in a domestic trade environment.

While criminal proceeds often need to be transferred to another country, a criminal transaction must be settled or funds must at some time come back to the criminal. These are reasons for criminals to move capital with the capabilities and constructed legitimacy of international trade. The techniques discussed hereafter have two things in common:

- The aim is to disguise criminal proceeds and move value across national boundaries, in an attempt to legitimise illicit origins of the value.
- It takes two parties to do so, and therefore there will be collusion between the exporter and importer, or both of them will be controlled by the same individual or entity.

Criminal financing

Goods that have either been purchased with the proceeds of crime (usually cash) or actually stolen are exported without the criminal origin of such goods being known to the relevant authorities in the originating and/or the destination countries.

Over- and under-valuation

By making over- or under-valuations of imports or exports, capital can be moved and laundered in the form of goods or money flows. Over- or under-valuation may take the form of over- or under-invoicing regarding price, quantity, quality or a combination thereof.

	Method	Indicators	Transfer of value
Import	Over-invoicing	Unusually expensive imports	In money abroad to the exporter
	Under-invoicing	Unusually cheap imports	In goods to the homeland to the importer
Export	Over-invoicing	Unusually expensive exports	In money to the homeland to the exporter
	Under-invoicing	Unusually cheap exports	In goods abroad to the importer

False descriptions

The goods identified on the invoice may not be the goods actually imported or exported. The documents can contain a price that corresponds to the specified goods but the actual market value of the goods imported or exported may be many times higher or lower. Physical observation is necessary in order to confirm that the goods shipped are the same as the goods invoiced. Goods shipped may actually be strategic goods, goods with restrictions (quotas), goods with a higher import duty or prohibited goods such as raw materials for drugs, weapons and fictitious goods.

Multiple billing

Multiple billing (or multiple invoicing) is a technique where multiple invoices are created for the same goods. This technique is used to justify multiple payments for the same shipment of goods.

Fictitious transactions

Lastly, transactions can be fictitious. The goods are never delivered or the services are never performed. Yet, with an invoice on hand, funds can be transferred or received. This serves to move money safely through corporate accounts, to falsify profits, to cover up or settle possible illegal activities. With current technology, it is easy to modify existing invoices or produce fictitious invoices. Information on corporations that is needed to create an invoice is readily available. It is also easy to set up a foreign corporation to deliver or receive goods or services when, in fact, they are neither delivered nor received.

Indicators

Unusual origin or destination of goods

- Country is not known for importing or exporting that type of goods
- Transactions with individuals or entities located in countries of risk

Unusual supplier or buyer

- Newly formed corporations with large imports and exports
- Volume or type of goods does not fit suppliers' or buyers' profile
- Offshore companies as suppliers or buyers

Unusual transportation of goods

- High costs of transportation compared to the value of the goods
- Size and weight or nature of goods does not fit in the method of transportation

Unusual description of goods

- Major differences between customs filings and invoices
- Major differences between description of goods on the invoice and the actual goods transported
- Risky goods: high value goods

Unusual pricing

- Major difference between declared value and market value
- Major difference between insured value and invoice

Unusual financing/payments

- Goods are purchased with funds of unknown origin (cash)
- A difference between the origin of the goods and the destination of the money (or vice versa)
- A difference between the amount of money paid and the amount invoiced
- A payment made by an offshore company or from an offshore account
- Commission payments to a third party without supporting documentation or economic justification
- Payments of goods are (partly) made by a third party and not the importer

Example

Figure 11 illustrates an example of how criminals employ the under- invoicing technique in order to disguise their criminal proceeds and move value through trade transactions, and legitimise the illicit origins of the value.

Figure 11. Trade-based money laundering - invoicing

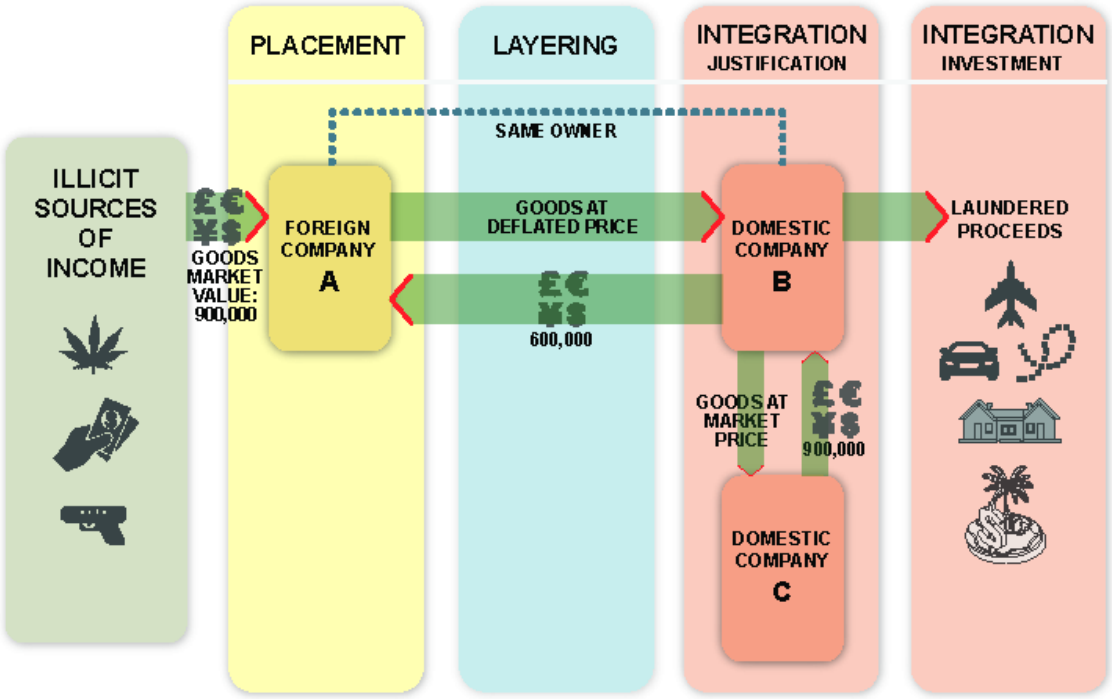


Figure 11 shows a stolen goods case with a fair market value of USD 900 000. These goods are exported to Domestic Company B (importer) with an under- invoiced amount of USD 600 000 from Foreign Company A (owner and exporter).

Domestic Company B, in turn, immediately sells them to an unrelated Domestic Company C at a fair market value price of USD 900 000. Through the course of this transaction, Domestic Company B has successfully laundered and justified the whole of the USD 900 000, as the total amount appears legitimate to the tax administration. At the same time, Domestic Company B shifted a value of USD 600 000 in cash to Foreign Company A.

Indicators for Loans

Introduction

Loans are primarily of interest for tax purposes where there are visible affiliated relationships which lead to questions about the shifting of profits, limiting of interest deductibility and the placement of informal capital. In relationships that are not visible or non-affiliated, loans can also be interesting from a tax point of view. The relevant factors for tax purposes are:

- The existence of a loan
- The qualification of the loan as a loan or as informal capital
- The deductibility of interest and, in doubtful debts, the deductibility of the principal amount.

Loan structures are widely used to launder criminal funds by disguising the criminal origin of the funds. Criminal money which is concealed or income from drug trafficking can be used to finance real estate or finance the operation of a company without taxation. The relevant factors for money laundering are:

- The existence of a loan
- The criminal origin of the funds
- Knowledge about the criminal origin

A structure with loans is simple and inexpensive to set up. The most common loan structures in which criminally obtained money plays a role are briefly discussed below.

Loan back

The loan back transaction is the best known form of money laundering by means of a loan and is the one most likely to be encountered. Through this arrangement one “borrows” one’s own criminal money back without it being visible to the outsider. This is done by creating a loan agreement with a “friendly relationship”, “family abroad” or “independent” offshore companies. The most common lender in this context is the foreign offshore corporation that has a bank account in a country with strict banking secrecy laws.

Back-to-back loan

In a back-to-back loan, illicit funds are first deposited into a bank account of a foreign company beneficially owned by the criminal. The criminal will then approach a lending financial institution (note they are usually unaware of the laundering) for the loan in the amount he is trying to launder and offer the funds of the foreign company as collateral. In most cases, early into repaying the loan, the criminal will then default on the loan. The recourse of the financial institution is to obtain the collateral from the criminal’s foreign company.

Criminal interference

In addition to the real involvement of one party (loan-back) or two parties (back-to-back) there may also be a criminal third party – in the background – that plays a role. This criminal interference achieves the financing of legitimate business activities through loans, supply of capital or comingling of illegal funds and legal funds. For example a criminal with cash proceeds of crime makes it available to legal Entity A, with the request to provide a loan from its own resources to Entity B. The criminal's cash serves as a guarantee or collateral for lender Entity A. The criminal obtains – without being visible – the investment or other use of the funds through Entity B.

Indicators

Unusual origin of the flow of funds

- Countries with strict banking secrecy laws and/or offshore financial centres
- Money flow is not from the country of the lender
- Money flows through a third party trust account for no apparent reason

Unusual lender and/or collateral provider

- Non-transparent (ownership of the) lender or the collateral provider
- Lender is a non-financial institution (not related to borrower)
- The lender or the collateral provider is from a country with an offshore financial centre or a country with strict banking secrecy laws

Unusual financing

- No alternatives for financing are being explored
- Unusual contracting partner/no business or family ties with country of origin
- Absence of supporting documentation between contracting parties
- No written loan agreement
- Absence or lack of sufficient collateral
- No or unrealistic repayment schedule
- Interest rate differs significantly from the market rate
- Loan comes in cash
- Nature of the use of the funds by the borrower
- Interest payments and repayments do not occur, schedules are not being respected and default occurs
- No measures for debt collection are taken
- Repayment is made without an actual flow of money to the lender
- Large write-off by the lender either shortly after granting the loan or after years and the security provided was insufficient

Unusual borrower

- Borrower with a low income compared to the loan and mortgage obligations
- Borrower with criminal records or background

Unusual user of assets funded

- Lack of income in relation to rent at market rate
- Persons with criminal records or background
- Social network of criminals

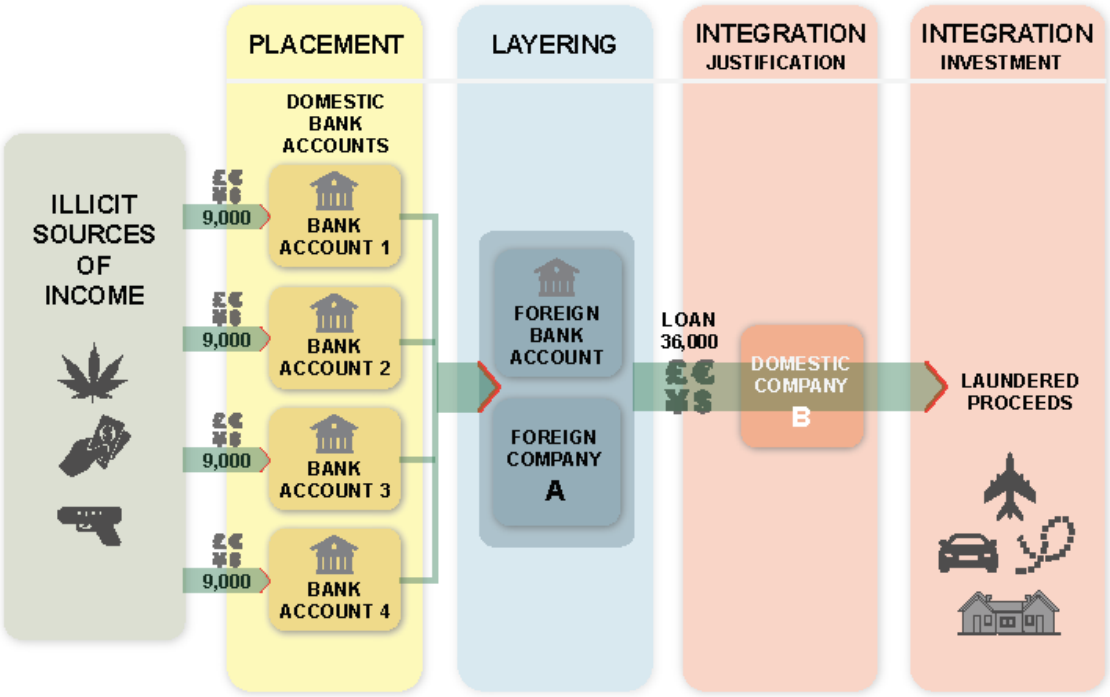
Unusual statements

- No explanation given, incomplete, unlikely or partly incorrect
- Explanation given is not easily verifiable

Examples

Loan back money laundering

Figure 12. Loan back money laundering



In this example, the criminal is holding large sums of cash he or she wishes to launder. This cash is deposited in various bank accounts in amounts that will not attract the attention of regulators. These amounts are then wired to a foreign bank where they are consolidated in an account controlled by foreign

Company A which is in turn controlled by the criminal. These funds are loaned back to the criminal's domestic Company B for use by the criminal. The source of these funds appears on the books of Company B as a loan payable to Company A.

Use of ostensible loans

During a tax audit of a company, the auditor noted questionable transactions between the company and one of its clients, a telecom company. The telecom company purchased various services (e.g. cleaning, renting of staff) from the company under audit. The presumably overvalued transactions as well as the transfer of funds were routed through an accounting firm owned by the same individual Mr X, who owned the company under audit.

A suspicion arose that Mr X now would have illicit funds (derived from tax fraud) available that needed to be laundered. Further analysis uncovered that Mr X never took direct "hands-on" control over the funds. He structured the transactions and money flows as a series of transactions between what was presented as third parties. With the funds already placed into the financial system (e.g. the bank account of the company under audit), the illicit funds were moved from the bank account from the company under audit to the bank account of a sub-contractor in the disguise of payments for services. Subsequently, the sub-contractor moved these funds to five individuals as "personal loan re-payments". These individuals used the same re-payment scheme towards Mr X, with each individual retaining 1% as their fee. The laundered funds were now in the hands of the owner (Mr X) and available for use.

Indicators for Professional Service Providers

Introduction

Professional service providers are corporations or individuals (entrepreneurs) who provide specialised services, which can include:

Legal service providers:

- Legal advice
- Legal assistance

Financial service providers:

- Advice in tax matters
- Completion of tax returns
- Bookkeeping, preparing and auditing the company accounts
- Private or personal banker

Trust or company service providers:

- Forming and selling corporations or other legal persons
- Acting or arranging for another person to act as a director or secretary of a company
- Providing a registered office, business address, correspondence or administrative address
- Acting as a trustee or a similar legal arrangement
- Acting as a nominee company director, secretary or shareholder for the ultimate beneficial owner

A criminal will at some stage require the expertise of a professional service provider. The involvement of a professional service provider is legally required in certain transactions, for instance, the services of a notary when completing a real estate transaction. The involvement of a professional service provider in a transaction is attractive for criminals because of:

- The nature of the services rendered which might assist in the money laundering process
- The name and reputation of an industry or group of professionals which raises confidence and gives the transaction a certain appearance of legitimacy
- The confidentiality maintained by certain professional service providers
- The third party trust accounts available from certain professional service providers.

Criminals may request services from unsuspecting professional service providers. There are, on the other hand, professional service providers who will knowingly provide services for criminals to help them conceal the flow of criminal money.

Indicators

Unusual service provided by a professional service provider

- Rendering services not being part of a day-to-day business
- Using the escrow account for non-related business transactions

Unusual professional service provider chosen for service

- Geographical distance between client and professional service provider is very large
- The services asked for exceed the volume the professional service provider usually renders

Unusual reward for a professional service provider

- Unusually high remunerations for services
- Remuneration comes in unusual kind

Unusual transaction, income or assets of the professional service provider

- Transactions not typical for day-to-day activities, regular income, assets or spending patterns
- Unusual private transactions or increase in wealth

Example

Unusual parties to the transaction

Company Y from offshore destination X holds a securities account at a bank institute in Country A. The ultimate beneficial owner of Company Y is an individual from Country B. In this securities account, shares are held which are listed at the Stock Exchange of Country B. Company Z from Country B wants to buy some of the shares held by Company Y; however, for unknown reasons, refuses to buy them from the offshore Company Y directly. Therefore, employees of the bank in Country A buy the shares from Company Y on behalf of the bank and resell them immediately to Company Z.

Although Company Z does not want to buy the shares from Company Y directly, the bank employees make it possible for the transaction to take place anyway. This is unusual.

The supervisor of Company A submits an STR to Country A's FIU, which reports the information to the tax administration of Country A. As a result of this, the involved employees of the bank are fired, they are taxed on the payment received for making the transaction possible and Country A's tax administration spontaneously shares their information with Country B.

Terrorist Financing Indicators

Indicators for Individuals

Introduction

This chapter focuses on terrorist financing indicators and behaviours of individuals that tax auditors and tax administrators may observe during their day-to-day activities. It does this by breaking down terrorist financing into three broad participant categories: 1) financiers and supporters; 2) organisers and operators; and 3) actors and executors. The categories are presented in the order thought most likely to be encountered by tax administrations.

Most tax administrations' efforts are primarily examining or auditing historical documents and previously filed tax returns. Therefore, tax examiners or tax auditors are most likely to uncover the illicit activities of financiers/supporters and organisers/operators. Actors/executors, on the other hand, operate in "real time" and will have limited exposure to tax administrations, unless identified or targeted by other government partners.

Depending on the size and sophistication of the terrorist organisation or sub-group, participants may move between the three categories. Whether large or small, formally or informally organised – or even self-funded – terrorists need reliable and ongoing sources of financing. The terrorist financing process creates records and leaves evidence that can be observed, analysed and exploited – creating financial intelligence – which can in turn assist counter-terrorist authorities and authorities combatting terrorist financing in addressing this continuing threat.

Financiers and supporters

Financiers and supporters are those who provide funds (collected or donated) for a terrorist organisation or individual actors. These may include funds derived from legitimate businesses, donations from charities and non-profit organisations, or illicit proceeds of criminal activity. The financiers/supporters may be unwitting or witting as to the terrorism nexus. While an element of secrecy may exist regarding the ultimate purpose or destination of the funds, evidence of their movement through the financiers/supporters' hands should be visible to the tax administration on some level.

Indicators for financiers and supporters

Financial activity

- Misuse of social benefits or questionable tax refunds claimed
- Receipt of financial support (or paid-for expenses and assets) from an unexpected or undefined source
- Fund transfers to or from conflict zones or neighbouring regions
- ATM transactions in conflict zones or neighbouring regions

- Movement of funds entirely unrelated to employment or other financial arrangements
- Credit cards which are close to or at their limit as a result of cash withdrawals
- Accumulating loans from various providers, in a short time period, with possible non-repayments
- Payments for travel to and from conflict zones or neighbouring regions
- Large or frequent donations to charities with connections to conflict zones or neighbouring regions
- Payments to media outlets or bookstores associated with propagating radicalism, extremism or violence (e.g. for the consumption or the creation of propaganda materials, printers, pamphlets, flags, etc.)
- A change in currency usage such as a sudden shift to financial instruments that are less transparent
- Use of wire transfers to or from countries of risk or between individuals located in the same jurisdiction, structured below required reporting amounts in attempts to avoid detection, or without a business purpose
- Power of attorney over a third party's bank account
- Loans made to persons without a business purpose (generally with no repayments)Donating funds to known extremist entities
- Payments made by means of encrypted money transfer applications (e.g. mobile messaging apps)
- Accumulating funds from various sources into one account with movement to one receiving account (e.g. Possible actor) either domestic or abroad
- Loans, lines of credit, and or credit card borrowing with no repayments
- Use of a letterbox company or companies
- Loans, lines of credit, or credit card borrowing with no repayments
- Buying or selling high value goods (e.g. cultural property) from conflict zones or neighbouring regions
- Buying or selling counterfeit goods
- Numerous loan applications
- High volume of cash deposits in excess of stated or known sources, particularly in personal accounts
- Deposit transactions made in location that is at a great geographical distance from where the accounts or owners are domiciled
- Unexpected amounts of cash held on business premises or domestic residence
- Rapid transfer or disbursement of funds following cash deposits

Personal behaviour

- Radicalisation (e.g. adopting a name related to extreme or fundamentalist groups or movement, sudden break in lifestyle or behaviour, conservative religious clothing, etc.)
- Exhibiting political or religious extremist views
- Criticism of government or government policy regarding terrorism-related issues, propagating radicalism, extremism or violence (e.g. observed through the individual's use of social media)
- Travelling to and from conflict zones or neighbouring regions
- Inclusion of the individual in a sanctions list
- Inclusion on a client list of tax preparer/accountant engaged in illicit refund schemes

Organisers and operators

Organisers and operators are those who are "managing" the terrorist organisation's (or sub-group's) activities. They are the strategic or tactical planners, overseeing one or more aspects of the organisation's efforts (e.g. recruiting, messaging, planning, procurement, directing operators and other subordinates, etc.) to further their goals and objectives. They will receive funds from, and may communicate with, the financiers; storing, moving, and using funds as needed.

Indicators for organisers and operators

Financial activity

- Fund transfers to or from conflict zones or neighbouring regions
- ATM transactions in conflict zones or neighbouring regions
- Movement of funds entirely unrelated to employment or other financial arrangements
- Credit cards, which are close to or at their limit as a result of cash withdrawals
- Payment for travel to and from conflict zones or neighbouring regions
- Payments for the development of special skills (e.g. pilot licences, fire arms licences, large vehicle/vessel licences etc.)
- Payments to media outlet or bookstores associated with propagating radicalism, extremism or violence (e.g. for the consumption or the creation of propaganda materials, printers, pamphlets, flags, etc.)
- Payments to rent "meeting type" spaces without an economic benefit or other logical explanation
- Loans or funds received from a third party without a business purpose (generally with no repayments)
- Payments made by means of encrypted money transfer applications (e.g. mobile messaging apps)
- Loans, lines of credit, and/or credit card borrowing with no repayments
- Real estate transactions funded by unknown sources
- Buying or selling high value goods (e.g. cultural property) from conflict zones
- Loans from a conflict zone or neighbouring region
- High volume of cash deposits in excess of stated or known sources, particularly in personal accounts
- Deposit transactions are located at a great geographical distance from where the accounts or owners are domiciled
- Tax refunds appear to be fictitious
- Unexpected amounts of cash held on business premises or domestic residence
- Cash withdrawals in countries of risk and surrounding borders
- Rapid transfer or disbursement of funds following cash deposits
- Questionable or fictitious business refunds to repeat customers (may indicate the movement of funds from a business to an individual or individuals in a terror cell)
- Use of wire transfers to or from countries of risk or between individuals located in these jurisdictions, of amounts below required reporting thresholds (in attempts to avoid detection)

- Purchase of dual-use goods (e.g. electronics, chemicals, weapons, training materials, survival materials, maps, GPS, PGP (encryption/decryption-enabled) smartphones, etc.)

Personal behaviour

- Radicalisation (e.g. adopting a name related to extreme or fundamentalist groups or movement, sudden break in lifestyle or behaviour, conservative religious clothing, etc.)
- Isolation from family, friends, work, or society in general
- Exhibiting political or religious extremist views
- Criticism of government or government policy regarding terrorism-related issues, propagating radicalism, extremism, or violence (e.g. observed through the individual's use of social media)
- Travelling to and from conflict zones or neighbouring regions
- Inclusion on a sanctions list
- Inclusion on client list of tax preparer/accountant engaged in illicit refund schemes

Actors and executors

Actors and executors are those who commit the terrorist act itself. This includes lone actors, home-grown violent extremists, foreign fighters (aspirational or returned), as well as sleeper cells of terrorists supported or directed by a designated terrorist organisation. Signs of self-radicalisation may be observed online through blogs, social media or even in the news. If such indicators are observed, tax examiners or tax auditors could, through management, refer to the appropriate authorities.

Indicators for actors and executors

Financial activity

- A significant change in tax filing pattern (e.g. gap in filing)
- Misuse of social benefits or questionable tax refunds claimed
- Receipt of financial support (or paid-for expenses and assets) from an unexpected or undefined source
- Large or frequent cash transactions, relative to income level (e.g. support from unrelated third parties)
- Fund transfers to or from and ATM transactions in conflict zones or neighbouring regions
- Credit cards which are close to or at their limit as a result of cash withdrawals
- Accumulating loans from various providers, in a short time period, with possible non-repayments
- Paying for travel to and from conflict zones or neighbouring regions
- Paying for developing special skills (e.g. pilot licences, firearms licences, large vehicle/vessel licences etc.)
- Loans or funds received from a third party without a business purpose (generally with no repayments)
- Loans, lines of credit, or credit card borrowing with no repayments
- Loans from a conflict zone or neighbouring region
- Numerous loan applications

- Fund transfers to or from and ATM transactions in conflict zones or neighbouring regions
- Payments made by means of encrypted money transfer applications (e.g. mobile messaging apps)
- Payments for extremist media outlets or bookshops
- Buying or selling counterfeit goods
- Cash deposits from unexplained sources
- High volume of cash deposits in excess of stated or known sources, particularly in personal accounts
- Deposit transactions are located at a great geographical distance from where the accounts or owners are domiciled
- Unexpected amounts of cash being held on business premises or at a residence
- Cash withdrawals in countries of risk and surrounding borders
- Rapid transfer or disbursement of funds following cash deposits
- Purchase of dual-use goods (e.g. electronics, chemicals, weapons, training materials, survival materials, maps, GPS, PGP (encryption/decryption-enabled) smartphones, etc.)

Personal behaviour

- Radicalisation (e.g. adopting a name related to an extreme or fundamentalist groups or movement, sudden break in lifestyle or behaviour, conservative religious clothing, etc.)
- Isolation from family, friends, work, society in general
- Exhibiting political or religious extremist views
- Criticism of government or government policy regarding terrorism-related issues; propagating radicalism, extremism or violence (e.g. observed through the individual's use of social media)
- Travelling to and from conflict zones or neighbouring regions
- Inclusion on a sanctions list
- Inclusion on a client list of tax preparer/accountant engaged in illicit refund schemes

Examples

Significant change in filing history or pattern

Significant changes in the tax filing history or pattern of filing of a person or that of a legal entity owned by the individual is an indicator to be mindful of when conducting a tax return examination or preparing for an audit. For example, in prior filings, an individual reports between USD 40 000-50 000 each year from their wage-earning job and has deductible expenses. However, the individual later reports USD 25 000 in wages, typical deductions, in addition to education expenses and unreimbursed business expenses that seem out of the ordinary and are not supported by the few records available to the tax examiner or tax auditor. This may indicate that the taxpayer is falsifying income and deductions to maximise the refund and that may then be used to fund suspicious activities, including money laundering and/or terrorist financing or another crime.

As a further example, an individual or legal entity has a pattern of having the tax refund deposited into a known financial account (e.g. a chequing account) but suddenly lists the card number of a pre-paid debit card instead. The tax examiner or tax auditor should discern if the change is based on a desire for anonymity or less scrutiny of the use of funds that would otherwise be evident in the known financial account.

Questionable refunds claimed

An individual files a false refund claim. He has falsely reported his income in an increased amount of USD 150 000 while claiming deductions for various categories of expenses (e.g. medical, childcare, donations, etc.). This is noteworthy as the individual is not known to have any children. Consequently, a refund is paid to him in the amount of USD 10 000. Making use of money transfers, this amount is then sent in smaller portions to a country neighbouring a conflict zone. An intermediary in that country then facilitates the delivery of the money to the individual's brother in a country where terrorist activity is taking place. This brother is a foreign fighter on behalf of a known terrorist organisation, which is on a sanction list.

At the outset, it may not have been apparent that any of preliminary facts relating to the case had anything to do with terrorist financing, However, one by one, newly obtained information by asking the right questions provided a picture of terrorist financing indicators, such as an attempt to conceal the magnitude of the total amount sent by sending sums below the amount required for reporting by the financial institution; the locale involved is a country neighbouring a conflict zone; the recipient of the wire transferred funds is a foreign fighter and associated with a terrorist organisation.

In another example, a potential foreign fighter (Mr D), age 28, was identified during the investigation of a travel facilitation network that sought to send individuals overseas to commit violent terrorist acts. Mr D was recruited and began training in the skills necessary to participate in violent terrorist activities overseas. The training included martial arts, firearm and knife training, language skills, and other topics.

In order to have funds available for when he was overseas, Mr D and others conspired to submit a false tax return for Mr D in which he falsely claimed that he lived with (another person's) three children and that they were his dependents. As a result of those false representations, Mr D obtained a tax refund in the amount of USD 5 587.

Embezzlement of government funding

A civil tax audit discovered an individual (Mr X) who used a company, where he was a board member, to raise funds that were subsequently suspected of being used in the funding of terrorism. The nature of the company was such that it received funding from the local government to promote the integration of new immigrants/individuals into society.

Mr X used his position to embezzle government funding from the company (the source of the terrorist financing), through a "gambling" account. From the gambling account he directed the funds to his personal account. Upon questioning, Mr X stated the money came from gambling winnings. The deposits into Mr X's personal account, which he claimed were "winnings", totalled EUR 20 000, EUR 130 000 and EUR 26 000 for 2014, 2015, and 2016, respectively.

Eventually, at the movement stage, the funds made their way to two distinct groups to be used. First, through analysis of Mr X's personal bank statements, tax officials noted he travelled in the refuge areas in the Balkans, Central Europe, and the Middle East. Secondly, as stated earlier, funds from the personal "gambling" account were funnelled to another account. The tax administration determined this personal account was used to fund the activities of ten unknown individuals, and one known individual (Mr Z). These transactions left a paper trail for tax officials to follow. Notably, tax officials observed the following:

- Bank statements indicating unusual amounts deposited into the personal account

- Questionable explanations of the source of funds deposited
- Tax returns indicating the income was not reported
- Bank statements also indicating other unusual transactions (e.g. questionable transfers to unknown account, purchase expenses indicating travel to high risk countries)

The tax administration examined the account of Mr Z further and found another source of deposits. A third individual who was a board member at a pre-school was also embezzling funds from the pre-school, and transferring them to the same account used by Mr Z. This led to the analysis of the bank statements of the pre-school, where the authorities observed large amounts of cash withdrawals and purchases seemingly unconnected to the pre-school.

Suspicious property investment

Customs authorities discovered an unusual amount of bank statements on an individual (Mr A) travelling to a country neighbouring a conflict zone. A referral was made to the tax authorities under the suspicion of tax evasion.

The tax authorities conducted a civil audit which eventually included an in-depth review of Mr A's financial situation. In his interview with tax authorities, Mr A said he had entered into a "business" arrangement with a third party (Mr B) to search out potential properties (in high risk conflict zones) for Mr B to invest in.

As part of the arrangement, Mr B would make large wire transfers (EUR 1 million over the last decade) into Mr A's bank account to be used for property investment. For his part, Mr A would receive an annual "commission fee for financial services" of EUR 5 000, plus any interest earned from the funds within Mr A's bank account. By his own admission, Mr A had no previous real estate business purchasing experience.

Based on these unusual facts, the tax authorities are considering a referral to the appropriate terrorist financing authorities. They determined there were no real property transactions but many transfers from Mr B to unknown parties in the high risk conflict zones via Mr A.

Indicators for Business

Introduction

The use of businesses (e.g., corporations, LLCs, partnerships, and sole proprietorships) in the financing of terrorist activities cannot be overlooked. Businesses can be used as a source which generates funds (legally and/or illegally) to be used to finance terrorism. They can also be a conduit for the movement of both funds and supplies (e.g. through trade-based transactions) that facilitate terrorist activities. In the course of the audit of a business, it is important to be aware of these two points when examining the business as well as its transactions.

Indicators

Unusual transactions and parties

- Transactions (e.g. shipments, wire-transfer, money transfer, cash courier) with parties located in conflict zones and nearby regions
- Fund transfers outside of regulated financial institutions (e.g. hawala and other informal value transfer systems)
- Fund transfers made by means of encrypted money transfer applications (e.g. mobile messaging apps)
- Transactions with unusual lender
- Questionable or fictitious business refunds to repeat customers (may indicate the movement of funds from a business to an individual or individuals in a terror cell)
- Risky goods such as high value goods and dual-use goods in unexpectedly high quantities

Unusual money flows

- Numerous incoming or outgoing money flows into business accounts with no apparent legitimate business purpose
- Lack of documentation regarding the purpose, source, or destination of the funds
- Rapid transfer or disbursement of funds following cash deposits
- Cash withdrawals in countries of risk and surrounding borders
- High volume of cash deposits in excess of stated or known sources
- Deposit transactions are located at a great geographical distance from where the accounts or owners are domiciled
- Indicators of other forms of fraud (e.g. Credit card, loans) such as questionable or unusual amount of credit card or loan applications
- Unexpected amounts of cash held on business premises or at a residence

Unusual business activity

- Purchase or storage of assets not related to the business (e.g. a print shop buying gas masks, encrypted phones, camping gear, fertilisers)
- Excessive purchase or storage of dual-use goods that are restricted or listed (e.g. radioactive material, chemicals and explosives)
- Unexplained inventory shortage of dual-use goods
- Sale of dual-use goods that are restricted or listed to unknown or unauthorised buyers
- Excessive cash deposits and other holdings not related to sales or debt
- Company assets used by unknown or unidentified individuals or entities without compensation

Unusual expenditures

- Paying for travel to and from conflict zones or neighbouring regions, for another person
- Large or frequent donations to charities with connections to conflict zones or neighbouring regions
- Assets paid for by the business which cannot be located or verified
- Advertising, publishing, printing expense invoices located and/or claimed, but not seen used in the business (possibly the creation of propaganda materials, e.g. printers, pamphlets, flags, etc.)
- Personal assets or expenses paid for by the business which do not appear to be used by the business owner

Examples

Company assets used by unknown/unidentified individuals or entities without compensation

It is a basic business assumption that assets will be put to their best economic use. The discovery of business assets that are used by persons with no connection to the business (or its principals or owners) and/or being utilised without reasonable compensation to the business is an indicator of possible terrorist financing efforts and, at a minimum, worthy of further inquiry.

A source of funding – refund

There are legitimate reasons why a business may generate a refund whether it is for sales taxes (GST/VAT), income tax or both. For example, one could expect to observe refunds claimed in the early years upon starting up a new business. However, where refunds are suspected of having been "manufactured", tax authorities may consider the possibility that these were used or might be used for terrorist financing. For example, indicators that may be observed that point to fictitious refunds include:

- Unsupported or fictitious expenses with companies in countries of risk (they may act to create a business loss as well as create possible fictitious tax credits that can be claimed against VAT). Furthermore, such fictitious expenses may mean funds are also moved to countries of risk.
- Suppression of reported sales where it appears that the business owner is not benefiting. Not only can this suppression help in creating a fictitious refund, it also may signal money being used directly for terrorist financing rather than for the benefit of the business owner.

Payments for products or services are received from multiple entities from offshore jurisdictions

A corporate restructure of Company A occurred during the period under review by a tax administration in Country A, which resulted in the formation of new trading entities. Documentation indicated that goods were supplied predominantly to one offshore entity located in a single jurisdiction. However, payments for the goods were received from multiple entities located in a range of offshore jurisdictions, including shell companies domiciled in high risk jurisdictions. There was evidence of a fabrication of export documents as they were generated or altered on the Customs reporting system well after the goods were shipped (possibly in response to requests for information from the respective tax administration in Country A). There were regular adjustments to the price of exported goods with regular refund claims being made. The veracity of these claims was considered to be questionable. Funds were channelled into and out of Country A through two money remitters and offshore trusts, in the absence of economic activity associated with the business. Wealth accumulated by individuals associated with Company A could not be explained and was not attributable to the export activity. Furthermore, Company A operated in a sector at high risk for bribery.

Purchase of unreasonable amount of fertiliser

An individual (Mr F) is excluded from a right-wing political party's youth movement due to his extreme tendencies and expressions. He has limited social interactions but is active in social media and gaming communities. Mr F is also suspected to be involved in fraudulent activities (internet sales of false documents and investments in the financial market). The proceeds of these suspected illicit activities are moved into a personal company.

Through this company, Mr F buys a small, remotely placed farm where preparations can take place undisturbed. He operates the farm entirely on his own, apparently without any professional skills/education. He buys a model of van seldom used by farmers. Mr F uses the company to acquire 6 000 kg of fertiliser from a local source; and, from several foreign sources, imports chemicals to convert the fertiliser into explosives. Mr F used his membership in a gun club to acquire hand guns, shotguns, and semi-automatic rifles.

A tax audit could have revealed the following terrorism indicators:

Indicators	Source
Unknown or suspicious source of funds used for farm purchase	Company & personal tax returns, bank records
Lack of prior farming or business experience	Farmers registry and company listings
Operating a farm or business without employees	Farm, company and personal tax returns
Unusually large fertiliser purchases for the size of farm	Accountancy and sales reports
Imports of chemicals from abroad (esp. if available domestically)	Customs or importing reports, accountancy & bank records
Possession of guns and licenses	Police records, gun registry

In many countries, sales of fertilisers are regulated, as they can be mixed with diesel to create ammonium-nitrate/fuel oil bombs. There are often similar requirements for retailers to report suspicious activities or large quantities related to certain chemicals, industrial gases, explosives, firearms and ammunition, and other hazardous materials.

Indicators for Charities and Non-profit Organisations

Introduction

Charities and non-profit organisations are vulnerable to being used, wittingly or unwittingly, to receive and disburse funds in support of criminal activities, including terrorist financing. Although the number of charities and non-profit organisations involved in terrorist financing represents a very small percentage of the non-profit sector, tax examiners and tax auditors should be aware that these sectors are high risk.

Indicators

Unusual transactions and parties

- Donations received from a state sponsor of terrorism or foreign entities located in or near a conflict zone, especially in the absence of a clear relationship or supporting documents
- Cumulatively large and not adequately justified amounts of donations, especially if made primarily in cash
- Use of the funds for expenditures which are not connected with the activity of non-profit organisations
- Money transfers to jurisdictions with no connection to the affairs of the charity or non-profit organisations
- Actual expenditures for goods are different from invoices or shipping labels
- Entity presents itself as a charity, but operates in an unregistered capacity to avoid regulatory scrutiny
- Principals, key employees, or large donors previously involved in other suspected or sanctioned charities
- Principals, key employees, or large donors are the subject of adverse or negative open source information
- Associated foreign entities, agents, or employees are the subject of adverse or negative open source information
- Transfer of funds or other assets to entities located/operating in or near conflict zones, especially when no activities or programmes in the areas have been reported
- Association by principals, directors, officers, key employees, or agents of a charity/non-profit organisation with organisations or individuals of interest relating to terrorism
- Disseminating/distributing/publishing extremist ideologies or materials via internet or other media

Indicators for Cryptocurrencies

Introduction

While cryptocurrency adoption and use is increasing, the use of these virtual value transfer systems for terrorist financing purposes has not been observed on a large scale. A few internet-based appeals for financial support of terrorist organisations have sought donations in the form of Bitcoin or other cryptocurrencies. These "donations" have involved only very small amounts of coins. The typically adverse physical/environmental conditions present in conflict zones (e.g. lack of electricity, internet access, violence, lack of resources to buy, etc.) inhibit cryptocurrency use.

In developed countries with stable infrastructure and economic conditions, cryptocurrencies may be used to collect, store, move, and possibly use goods and services in support of terrorist aims and operations. However, tax examiners and tax auditors will likely not observe indicators of such activities as most of them take place on the dark web. For example, calls for cryptocurrency donations to facilitate terror activity have been found on the dark web. Moreover, many items that could easily be used to assist in promoting terror attacks (e.g. fake passports, social security cards, weapons) can easily be found on the dark web.

Cryptocurrencies can be used to help facilitate the collecting stage of terrorist financing. While the use of cryptocurrencies may not be widespread, there are individuals who will seek out ways to use cryptocurrencies at the various stages of terrorist financing and thus, tax examiners and tax auditors must remain vigilant in recognising the mixing of indicators.

Indicators

Unusual origin

- Receipt of cryptocurrencies from individuals, entities, or locations associated with terrorism or conflict zones and neighbouring areas

Unusual transactions

- Transfer of cryptocurrencies or wallets to persons or organisations linked to conflict zones and their neighbouring areas
- Cryptocurrency purchases of dual-use goods, camping/survival/medical equipment
- Directed delivery of such cryptocurrency purchases to conflict zones and their neighbouring areas

Example

The importance of seeing the big picture

The following example highlights the importance of seeing the big picture and all possible indicators when deciding on a referral to the appropriate law enforcement authorities.

Between March 2017 and the date of her attempted travel to Syria on 31 July 2017, a 27-year-old woman (Ms C) engaged in a scheme to defraud numerous US financial institutions. Specifically, Ms C obtained a loan for over USD 22 000 by way of materially false pretences, representations and promises. Ms C. also fraudulently applied for and used over a dozen credit cards, which she used to purchase approximately USD 62 000 in Bitcoin and other cryptocurrencies online. Ms C then engaged in a pattern of financial activity, culminating in several wire transactions totalling over USD 150 000 to individuals and shell entities that were fronts for foreign terrorist organisations.

While this case was ultimately detected and investigated by law enforcement authorities, there was a paper-trail of indicators that tax examiners or tax auditors could have observed, including:

- Unusually large amounts of paperwork related to different credit cards
- Credit card obtained for specific/targeted purpose (e.g. to purchase cryptocurrency)
- Paper wallet holding a private key to the bitcoins
- Unusual paperwork related to the loan
- Bank statements indicating unusual transactions (e.g. questionable sources, relatively quick in and out transactions, offshore transfers to high risk countries)

Useful Resources

The FATF website (www.fatf-gafi.org), the World Bank website (www.worldbank.org), the International Monetary Fund website (www.imf.org) and the United Nations website (www.un.org) have additional materials on money laundering and terrorist financing.

Resources on Money Laundering

- FATF (2012-2018), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, www.fatf-gafi.org/recommendations.html

Resources on Terrorist Financing

- FATF (2008), Proliferation Financing Report, www.fatf-gafi.org/media/fatf/documents/reports/Typologies%20Report%20on%20Proliferation%20Financing.pdf
- FATF (2012-2018), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, Paris, www.fatf-gafi.org/recommendations.html
- FATF (2013), Money Laundering and Terrorist Financing; Vulnerabilities of Legal Professionals, www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20vulnerabilities%20legal%20professionals.pdf
- FATF (2014), Risk of terrorist abuse in non-profit organisations, FATF, Paris, www.fatf-gafi.org/media/fatf/documents/reports/Risk-of-terrorist-abuse-in-non-profit-organisations.pdf
- FATF (2015), Best practices on combating the abuse of non-profit organisations - recommendation 8, FATF, Paris, www.fatf-gafi.org/media/fatf/documents/reports/BPP-combating-abuse-non-profit-organisations.pdf
- FATF (2015), Emerging Terrorist Financing Risks, FATF, Paris www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing- risks.html
- FATF (2015), Financing of the terrorist organisation Islamic State in Iraq and the Levant (ISIL), FATF, www.fatf-gafi.org/topics/methodsandtrends/documents/financing-of-terrorist-organisation-isil.html
- FATF-GIABA-GABAC (2016), Terrorist Financing in West and Central Africa, FATF, Paris www.fatf-gafi.org/publications/methodsandtrends/documents/terrorist-financing-west-central-africa.html

- FATF (2016), Guidance on the criminalisation of terrorist financing (Recommendation 5), FATF, Paris, www.fatf-gafi.org/publications/fatfrecommendations/documents/criminalising-terrorist-financing.html
- FATF (2018), Financing of Recruitment for Terrorist Purposes, FATF, Paris www.fatf-gafi.org/publications/methodsandtrends/documents/financing- recruitment-terrorist-purposes.html
- FATF (2018), Professional Money Laundering, FATF, Paris, www.fatf-gafi.org/media/fatf/documents/Professional-Money-Laundering.pdf
- The commission Regulation (EC) No 552/2009 of 22 June 2009 amending Regulation (EC) No 1907/2006 of the European Parliament and of the Council on the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH) as regards Annex XVII. This Annex sets out the list of restrictions on the manufacture, placing on the market and use of certain dangerous chemical substances, mixtures and articles.

Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors

Financial crimes, including tax evasion, money laundering, and terrorist financing undermine jurisdictions' political and economic interests and pose a serious threat to national security. Tax crime is a key source of dirty money and as such, tax authorities have a central role to play in identifying and reporting money laundering and terrorist financing. The purpose of this handbook is to raise the awareness level of tax examiners, auditors, and investigators, of their role in combatting these illegal activities.

OECD
BETTER POLICIES FOR BETTER LIVES

For more information:

OECD.TaxandCrime@oecd.org

www.oecd.org/tax/crime

@OECDtax