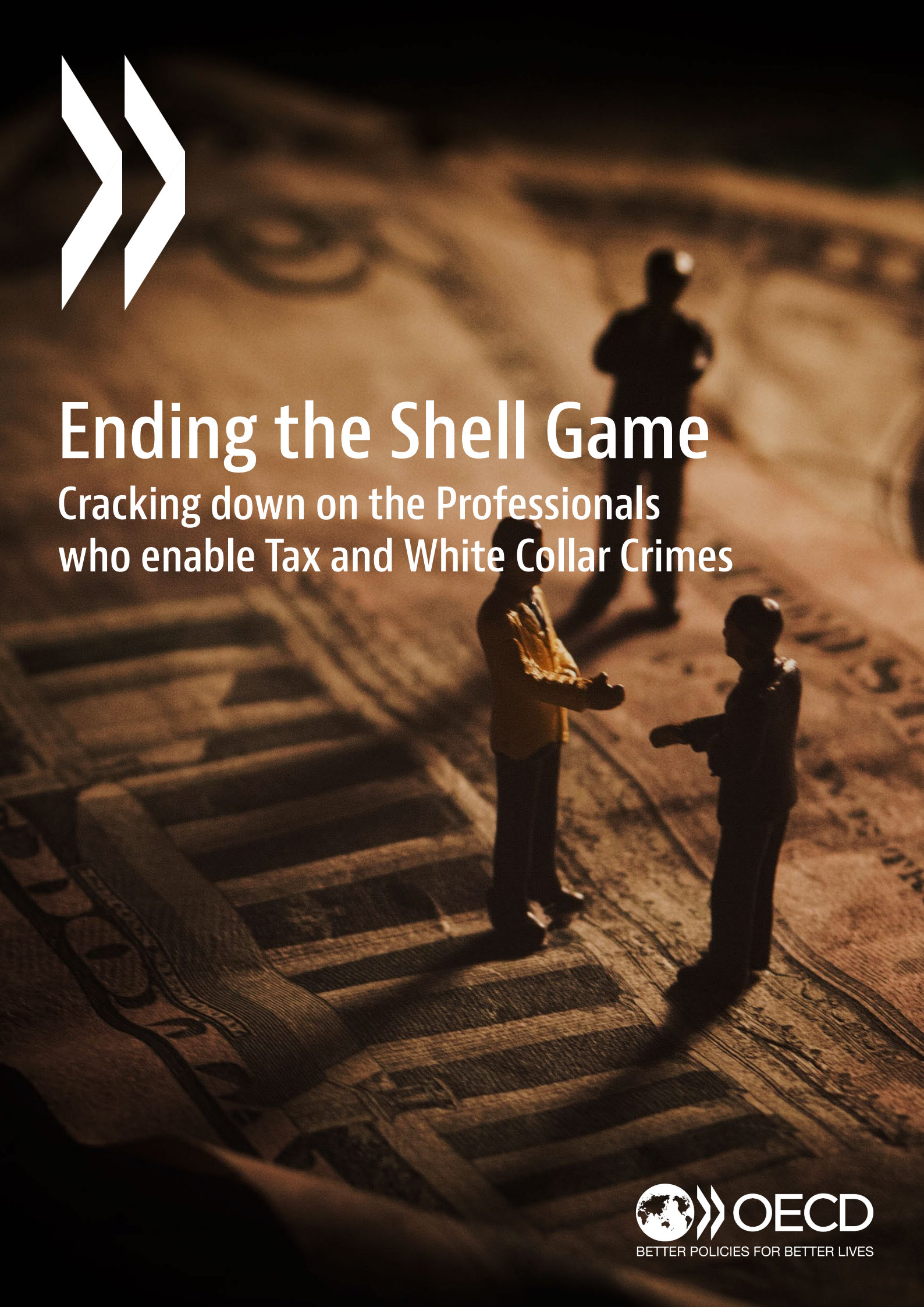


Ending the Shell Game

Cracking down on the Professionals who enable Tax and White Collar Crimes

OECD
BETTER POLICIES FOR BETTER LIVES

Ending the Shell Game: Cracking down on the Professionals who enable Tax and White Collar Crimes

This document was approved by the OECD Committee on Fiscal Affairs on 16 November 2020 and prepared for publication by the OECD Secretariat.

This document, as well as any data and 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.

Please cite this publication as:
OECD (2021), Ending the Shell Game: Cracking down on the Professionals who enable Tax and White Collar Crimes, OECD Publishing, Paris.
http://www.oecd.org/tax/crime/ending-the-shell-game-cracking-down-on-the-professionals-who-enable-tax-and-white-collar-crimes.htm

Photo credits: © Zenza Flarini – Shutterstock.com.

Corrigenda to OECD publications may be found on line at: *www.oecd.org/publishing/corrigenda*.

Table of contents

Boxes

Abbreviations and Acronyms

AEOI Standard	Standard for Automatic Exchange of Financial Account Information in Tax Matters
AML	Anti-Money Laundering
ATO	Australian Taxation Office
CIN	Corporate Identification Number
CMS	Crypto-asset Mixing Service
CRS	Common Reporting Standard
CTF	Counter-Terrorism Financing
DIN	Director Identity Number
DLG	JITSIC Data Leaks Group
DNFBP	Designated Non-Financial Businesses and Professions
DOJ	Department of Justice of the United States
EU	European Union
FATF	Financial Action Task Force
FIOD	Dutch Fiscal Intelligence and Investigation Service
Global Forum	Global Forum on Transparency and Exchange of Information for Tax Purposes
HMRC	Her Majesty's Revenue and Customs
IAD	Income and Asset Disclosure
ICAI	Institute of Chartered Accountants of India
ICIJ	International Consortium of Investigative Journalists
IDS	JITSIC Intermediaries Disruption Strategy
IESBA	International Ethics Standard Board for Accountants
IMF	International Monetary Fund
IRS	Internal Revenue Service of the United States
J5	Joint Chiefs of Global Tax Enforcement
JITSIC	Joint International Taskforce on Shared Intelligence and Collaboration
NECC	National Economic Crime Centre of the United Kingdom
NFRA	National Financial Reporting Authority of India

OECD	Organisation for Economic Co-operation and Development
PAN	Permanent Account Number
PEPs	Politically Exposed Persons
StAR	Stolen Asset Recovery Initiative
STR	Suspicious Transaction Report
TFTC	OECD Task Force on Tax Crimes and Other Crimes

Executive summary

Over the last decades, the world has witnessed increasingly sophisticated financial crimes being perpetrated across borders – and the public interest in addressing such issues has also grown, as has been evidenced in the media through widely publicised leaks such as the Panama and Paradise Papers (ICIJ, 2020[1]). These crimes are often facilitated by lawyers, accountants, financial institutions and other professionals who help engineer the legal and financial structures seen in complex tax evasion and financial crimes. The small segment of professionals that generate opportunities to facilitate the commission and / or concealment of such crimes undermine not only the rule of law, but their own profession, public confidence in the legal and financial system, as well as the level playing field between compliant and non-compliant taxpayers. Ultimately, this undermines the public interest in ensuring taxes are paid and available for public use. Therefore, targeting professional enablers and disrupting their activities is a key avenue for addressing criminal activity at the source.

The majority of professionals are law-abiding and play an important role in assisting businesses and individuals to understand and comply with the law and helping the financial system run smoothly. Such law-abiding professionals are to be differentiated from a small set of professionals who use their skills and knowledge of the law to actively promote, market and facilitate the commission of crimes by their clients. This report seeks to support policy makers and law enforcement authorities to address the actions of that small set of lawyers, tax advisors, notaries, financial institutions and other intermediaries that are "professional enablers," intent on facilitating wrong-doing by their clients.

Professional enablers play an integral role in making it easier for taxpayers to defraud the government and evade their tax obligations, such as by offering non-transparent structures and schemes to conceal the true identity of the individuals behind the illegal activities undertaken. This type of activity has become a subject of international and domestic political significance and been covered extensively in the media. These scandals also reveal the broader problem of tax evasion in society: that it undermines public confidence as well as the public purse, and gives rise to an increasing sense of instability caused by inequality. In the wake of the COVID-19 pandemic, emerging risks continue to come to light, such as the potential role of professional enablers in perpetrating fraudulent access to pandemic support funding. This highlights the persistent risk professional enablers create in society.

Governments have therefore recognised the need to target the professional enablers who actively pursue opportunities for, and conceal the commission of, tax crimes and other financial crimes, in order to disrupt a crucial part of the planning and pursuit of criminal activity. This is not the only strategy that is needed to address all tax and financial crimes; however, it is one that can be cost-effective by reducing the accessibility of sophisticated means of tax evasion and fraud, thereby narrowing the opportunities for such crimes to take place.

Countries have reported, however, that while they recognise the importance of the issue, there are challenges in being able to effectively tackle professional enablers. This report explores different governmental strategies to detect, deter and disrupt the activities of professional enablers.

This report

This report sets out actions governments can take to address the issue of professional enablers in five key areas:

1. Understanding the role of professional enablers;
2. Methods for identifying professional enablers;
3. Legal and regulatory frameworks to disrupt professional enablers;
4. Strategies for deterring professional enablers; and
5. Domestic and international multilateral efforts to address professional enablers.

While professional enablers include a wide range of individuals, intermediaries and institutions providing an array of services that may vary in specifics from one country to another, this report highlights the common approaches used in combatting the use of professional enablers. This report is primarily targeted at authorities with responsibility over tax crimes, but it is also intended to be helpful to other law enforcement authorities, given the links between tax offences and other financial crimes such as money laundering or corruption and the commonalities in the ways these crimes are committed, and particularly insofar as it outlines the importance of multi-agency and multilateral action.

This report has been prepared by the OECD Task Force on Tax Crimes and Other Crimes, drawing on the experience of both OECD and non-OECD member countries.

Conclusions and recommended counter-strategies to combat professional enablers

This report fosters better understanding of the problem posed by professional enablers and the range of actions that can be taken in response, with a view to encouraging countries to establish a dedicated national strategy to tackle professional enablers who actively participate in tax crimes and other financial crimes.

This report calls on countries to consider adopting a strategy, or strengthen their existing strategy, for addressing professional enablers. In devising or strengthening their national strategy, countries should consider the recommended counter-strategies to combat professional enablers outlined in Table 1 below.

Table 1. Recommended counter-strategies to combat professional enablers

Recommendation	Key elements
Awareness *Ensure tax crime investigators are equipped with the understanding, intelligence and analytics skills to identify the types of professional enablers operating in their jurisdiction, and to understand the risks posed by the ways that professional enablers devise, market, implement and conceal tax crime and financial crimes.*	• Consider the need for a common definition of professional enablers, recognising the role and different levels of culpability within different sectors • Educate across government agencies about the types of services provided by professional enablers and why they pose a risk • Develop risk indicators for identifying professional enablers, drawing on a wide range of available data sources

Legislation *Ensure the law provides investigators and prosecutors with sufficient authority to identify, prosecute and sanction professional enablers, so as to deter and penalise those found to be professional enablers of tax crime.*	• Consider whether there is a need for a specific professional enabler liability regime, to further deter this behaviour • Assess whether the legal framework provides sufficient ability for prosecutors to prove the offence of acting as a professional enabler • Reflect on whether professional privilege poses a barrier to successful investigation and prosecution • Consider whether the ability of suspects to settle cases hinders the deterrent effect of the law • Explore whether professional supervisory or regulatory bodies can be used to stop professional enablers from operating
Deterrence and disruption *Ensure there is a coherent and multi-disciplinary strategy for preventing and disrupting the behaviour of professional enablers, including engaging in communication, leveraging the role of supervisory bodies and industry sectors, incentivising early disclosure and whistle-blowing and taking a strong approach to enforcement in practice.*	• Prevent abuse through communication with taxpayers and education of professionals • Leverage the role of, and information available to, professional supervisory bodies and regulators • Incentivise good corporate governance and a culture of compliance • Create voluntary disclosure, reporting and whistle-blowing facilities • Consider introduction of mandatory disclosure rules to require intermediaries to report on possible schemes early in the life cycle
Co-operation *Ensure relevant authorities are proactively maximising the availability of information, intelligence and investigatory powers held by other domestic and international agencies to tackle professional enablers that are sophisticated and operating cross-border.*	• Use domestic whole of government mechanisms, such as reporting of suspicions, information sharing, cross-agency investigations, and other proactive co-operation mechanisms; • Use international co-operation mechanisms, including the broadest range of exchange of information (including on request and automatic, group requests, spontaneous exchange, and on-sharing with other agencies), as well as multilateral co-operation mechanisms.
Implementation *Appoint a lead person and agency in the jurisdiction with responsibility for overseeing the implementation of the professional enablers strategy, including to undertake a review of its effectiveness over time and devise further changes as necessary.*	• Secure commitment from senior leadership in policy and law enforcement agencies to address and tackle professional enablers, contribute to the strategy, and implement the relevant aspects of the strategy; • Appoint a national focal point who will liaise among different government agencies and assess the needs, challenges and strengths of each government agency in regards to tackling professional enablers; • Engage in open discussions across government, businesses, the public, academia and professional associations to draw on experiences and opinions from all sectors; • Ensure appropriate resources are provided for effective implementation of the professional enabler strategy.

1 The role of professional enablers in tax and other financial crimes

1.1. Who are professional enablers

In general, professional enablers of tax crime and other financial crimes are intermediaries with specialised knowledge who play a specific role to facilitate the commission of a tax offence (and possibly other related financial crimes) by others. Professional enablers of tax crime and other financial crimes can include for example: tax professionals, lawyers and legal advisors, accountants, financial advisors, banks and financial institutions, company formation agents, registered agents, notaries, business trustees, trust and corporate service providers, and other promoters of tax evasion schemes.

1. Law-abiding professionals performing their duties in accordance with the law are an important part of the legal and financial system, and help ensure compliance with the law. Professional enablers are a distinct segment of professionals that intentionally and actively devise strategies to facilitate the commission of crimes (whether serving both legitimate clients and those engaging in tax crimes or other financial crimes). This report focuses on professional enablers who serve criminal clients whether on a fulltime or part-time basis.

2. A professional enabler is typically an individual or entity with professional expertise to perform a specific service to aid their customer in carrying out a tax offence or other financial crime.[1] Most countries do not have a specific definition of a "professional enabler". However, the common attributes of a professional enabler include:

- Professional qualifications or training;
- Expertise in taxation, legal or financial processes;
- Experience in setting up tax structures, or structures with cross-border elements; and
- Experience setting up opaque structures for avoiding investigative scrutiny into the clients' tax and economic activities.

3. For some countries, the concept of a professional enabler can be narrow and focus on the most proactive, intentional conduct; while others take a broader view and include those that know or have reason to know that their services are being misused. For example, there can be distinctions between:

- General enablers of tax offences through the provision of services such as those outlined in section 1.2;
- Promoters of tax evasion that actively design and market tax evasion schemes;

[1] An example of both individuals and financial institutions being prosecuted as professional enablers can be found at Box 16.

- Facilitators and service providers that implement aspects of the tax evasion scheme, but who may have a different level of knowledge or expertise and whose involvement is only one part of the bigger picture.

Depending on the country, these distinctions can lead to separate tax offences, different amounts of penalties, the use of civil (non-criminal) sanctions, or the criminalisation of certain higher-level aggravated offences but not others.

4. Professionals offer various legitimate business services to clients such as legal and accounting advice. They may also be experts on finding legal loopholes giving room for the creation of "tax-avoidance" strategies. These strategies operate in the so-called "grey areas of the law", allowing professionals to use the inadequacies or ambiguities of a jurisdiction's legal framework to maximise the tax outcomes for their client. The possibility of using "grey areas of the law", while not technically illegal, should be limited by jurisdictions through the enhancement of their tax legislation and by fostering international co-operation. This is an area in which the OECD has been active over the years through the OECD/G20 Inclusive Framework on BEPS (OECD, 2020[2]),[2] and is not the focus of this report.

5. Rather, this report focusses on the situations when the services and advice provided by professionals go beyond the interpretation and search for legal loopholes, and reach the point where professionals enable the commission of tax fraud and tax evasion through active support and participation. The difference between legitimate legal counsel or professional advice, and participation in the commission of a crime, resides in the type of advice offered by the professional and whether illegal activities derive from it.

6. This report assumes a wide definition of such professional enablers, who have the hallmarks of being trained professionally or having specific expertise within key professions. Professional enablers are skilled professionals who use their knowledge for facilitating the commission of tax and economic crimes, usually in large scale and through sophisticated means. This wide definition of professional enablers allows authorities to develop a strategy that is comprehensive, both focussing on professional enablers of tax crime that are actively enabling the commission of tax offences, whilst also recognising that facilitators of tax crimes who are less cognisant of their complicity remain an issue (either by being wilfully blind or where they would reasonably be expected to know of the risks they pose).

1.2. Services provided by professional enablers

Professional enablers can offer a number of services, many of which are legitimate business services. However, these legitimate services can be used to facilitate the commission of tax crimes and other financial crimes.

7. The following examples illustrate the most common or problematic services provided by professional enablers as identified by the TFTC. The mere provision of these services is not an indication that the service provider is a professional enabler and several of these services themselves are not only legal, but essential parts of the global financial system. However, where it is combined with an intent that the service be a part of a scheme for committing a tax crime, or where the service provider is wilfully blind or would reasonably be expected to know that their services were being sought for this purpose, they may be a professional enabler.

[2] The OECD/G20 Inclusive Framework on BEPS has over 135 countries committed to tackling tax avoidance, improving the coherence of international tax rules and ensuring a more transparent tax environment.

8. While the types of illegal services provided by professional enablers vary in each jurisdiction, common trends emerge from comparative experience. Some examples include:

- Hiding income or disguising the character and source of profits, for the purpose of tax evasion;
- Obscuring beneficial ownership of assets, often through complex legal structures involving several jurisdictions, with the purpose of avoiding investigative scrutiny;
- Offering advice on how to evade tax obligations using falsified transactions, documents or filings.

9. The following sections outline different types of services identified by countries as common services provided by professional enablers. Many of these activities may not only facilitate tax crime, but also other financial crimes such as money laundering, necessitating multi-disciplinary approaches as discussed in chapter 5 below.

1.2.1. Setting up companies, trusts and other business structures

10. Most countries contributing to this report highlighted the prevalence of the companies, trusts and other corporate entities and arrangements in tax fraud and financial crime cases. Corporate structures are attractive to criminals for two main reasons: because they provide an air of legitimacy (IMF, 2019[3]); and, because they are separate from the individuals behind the corporate veil, they provide the ability to shield the identity of the beneficial owner, as discussed below (Halter et al., 2011[4]). For example, criminal funds can be disguised within legitimate business transactions by merging legal and illegal profits, which can be transferred either to other business entities or to domestic or foreign bank accounts. As such, professional services for the formation of such entities and arrangements, while itself an important and legal activity, can also be an area of interest for investigators where such vehicles are then used for illegal activities.

11. Use of business structures for illegal purposes is facilitated by an environment where quick, low-cost and easy incorporation is available. While the speed of incorporation is often designed to reduce the compliance burden on legitimate business owners and to encourage national economic growth, this can also create vulnerabilities to abuse by criminals. Easy availability or formation of new companies negates the need for criminals to infiltrate established businesses. In many cases, fraudsters make use of corporate structures spanning multiple jurisdictions in order to hinder investigations and to best present a legitimate front. For example, an onshore jurisdiction can be used when setting up the “front” company, whereas accounts and assets are then located in offshore jurisdictions. Furthermore, the choice of the type of legal entity can be deliberate, in order to exploit legal arrangements where the separation of legal ownership and beneficial ownership of assets is designed to pose an impediment to investigators identifying, or recovering assets from, the owner.

12. Several countries cited this as an area where they have specific projects looking into the use of company formation agents or trust and corporate service providers, due to the prevalence of these professional enablers in establishing the corporate structures used for tax evasion schemes or hiding beneficial ownership and income. Such professional enablers’ services can include for example:

- Assisting in the opening of shell companies by registering in the name of other legal persons, or assisting in the opening of bank accounts in names that obscure the ownership, both domestic and foreign;
- Safe custody of incriminating data;
- Managing or assisting in investing unaccounted funds which are the proceeds of crime in overseas jurisdictions;
- Referral services to other counterpart service providers, e.g. in an offshore jurisdiction, in order to create a cross-border structure which makes detection by law enforcement authorities more difficult.

Box 1. Foreign trusts used in ownership chains to hide beneficial ownership and financial flows

This example is provided by New Zealand

In the wake of certain revelations in the Panama Papers, New Zealand became aware of the possible misuse of New Zealand trusts by trust and company service providers. This misuse was centred on shielding the beneficial ownership of the ultimate controllers, whilst trading off New Zealand's good reputation internationally as a robustly regulated jurisdiction. Thus, New Zealand trusts were being interposed as a further layer in international chains of ownership to make it more difficult for authorities to readily trace both ultimate beneficial ownership and financial flows, and this activity was enabled by trust and company service providers through the establishment and administration of foreign trusts.

Once this information came to light, the New Zealand government moved quickly to strengthen the disclosure rules for foreign trusts. New rules were introduced to require foreign trusts (i.e. trusts settled by non-residents) to be registered with Inland Revenue, including full particulars of settlors, trustees, beneficiaries or persons with power in relation to the trust or trustee. Trust deeds and supporting or amending documentation must also be provided on registration. There is an ongoing obligation to provide full details of settlements on the trust to Inland Revenue, along with annual disclosures to maintain registration as a foreign trust.

The information collected under these new rules is stored in a register maintained by Inland Revenue. This information can be shared with the Police Financial Intelligence Unit, as well as the Department of Internal Affairs, which supervises trust and company service providers for anti-money laundering purposes. Relevant details of foreign trusts are also provided to New Zealand's tax treaty partners on request under exchange of information instruments.

The introduction of these strengthened disclosure requirements for foreign trusts was designed to provide the transparency necessary to deter misuse of foreign trusts, particularly by those trust and company service providers relying on light disclosure to be effective. These predictions have proven to be correct with a major reduction in the number of foreign trusts now administered in New Zealand – a full 75% decline in the number of foreign trusts from 11 671 (as at 31 May 2016) to 2 965 (as at 31 May 2019).

1.2.2. Setting up offshore structures to hide beneficial ownership and income

13. Professional enablers are commonly cited as a concern in connection with their involvement in the establishment of offshore structures. In particular, offshore structures can be utilised to hide beneficial ownership or income / assets. Offshore structures to obscure the beneficial ownership can be used, for example, to conceal the proceeds of crime (such as income on which tax is evaded, or a bribe), or to attempt to evade tax reporting obligations (such as under the Standard for Automatic Exchange of Financial Account Information in Tax Matters (AEOI Standard)). Where a number of corporate entities or arrangements are interposed in different jurisdictions, such as a string of shell companies with complex ownership and control structures, it makes it more difficult for investigators to quickly and accurately identify the person who owns the assets and, if that person is a criminal offender, to recover those assets.

14. Countries have also cited that professional enablers specifically facilitate the creation of instruments that can be used to obscure beneficial ownership such as bearer shares and nominee directors or shareholders. In these cases, the professional involved is key to enabling the creation of these instruments to be used to conceal the identity of those involved in tax or other financial crimes. An example of this can be where "dummy" directors, trustees, shareholders etc. are provided by the professional enabler to disguise their client's beneficial ownership. The simplest use of a nominee carries the risk of

significantly obscuring the beneficial ownership of the entity or assets. This is because nominee arrangements are often private agreements between individuals, and the existence of the arrangement may not be apparent to an investigator. Furthermore, a nominee can itself be a company, which adds a further layer of opacity and complexity for investigators seeking to identify the persons with the ultimate ownership and control. Use of nominee directorships can therefore be viewed as a risk indicator for criminal activity and professional enablers.

Box 2. Dividend structure to obscure beneficial ownership and investment income offshore

This example is provided by the Netherlands

A Dutch taxpayer engages in an aggressive tax planning structure. The taxpayer sells his sole proprietorship of a closely held business to an alleged third party. This third party is often a Dutch legal entity whose shares are held by an entity established in an offshore jurisdiction, which is actually managed by the Dutch taxpayer through nominee directors. Payments are made from the offshore entity to the ultimate beneficial owner; however, the payments are disguised as gifts or loans with favourable loan conditions instead of a dividend payment that would normally have taxation implications. This entire scheme is perpetrated by the Dutch taxpayer to deliberately conceal and evade taxes on taxable dividend payments.

As the amounts are transferred to a foreign bank account of the ultimate beneficial owner and the foreign bank account is not declared in the Dutch taxpayer's income tax return, the Dutch tax authorities are not able to detect the tax evasion unless they receive intelligence on the tax evasion scheme, such as information on the Dutch taxpayer's foreign bank account received through the Automatic Exchange of Financial Account Information in Tax Matters.

Box 3. Professional enablers setting up offshore structures targeted in a sting operation

This example is provided by the United States of America (DOJ, 2014[5])*

Company A, a boutique investment company based in an offshore jurisdiction, was involved with money management and investment strategies for high net worth individuals. Government officials received information suggesting the investment firm was recruiting United States citizens to invest offshore. It was unknown whether Company A was instructing the US citizens to report the offshore accounts to the government, as legally required.

Undercover agents contacted Company A's investment advisors and communicated they were interested in investing offshore, and wished to meet in person to discuss some of the "sensitive" money they controlled. The undercover agents told the investment advisors that they had orchestrated a bank fraud scheme and therefore had USD 2 million they needed to move offshore to avoid a bank's "lookback period audit" and evade detection from law enforcement officials.

The investment advisors said they typically did not take US clients, but encouraged the officials to meet with an attorney in another offshore jurisdiction to create an offshore foundation. Therefore, it would be the offshore foundation that would become their client and not the US citizens, and the offshore foundation would serve as an entity to conceal true beneficial ownership.

These undercover agents travelled to this other offshore jurisdiction and paid USD 5 000 to create an offshore entity. Subsequently, funds were transferred from the United States to the first offshore

jurisdiction where the funds were commingled with other corporate accounts, before being transferred to the second offshore jurisdiction under the management of Company A. Throughout this operation, Company A's investment advisors were fully aware of their role in managing funds that were untaxed and proceeds of a purported bank fraud.

After a few months, the officials contacted the investment advisors to say they were interested in liquidating their account. The funds were diverted through their offshore entity and returned to their home country, committing money-laundering offences as the investment advisors knowingly invested "dirty money" and used a shell corporation to conceal the true origin and ownership of the funds.

When arrests were made, those arrested co-operated with government officials. The subjects were sentenced to federal prison and spin-off investigations were developed based on the intelligence provided by the professional enablers. Observations and learnings include that targeting the promoters of fraud is much more beneficial and leads to more wide reaching investigatory outcomes than targeting individual investors moving money overseas.

* Note: This example is provided through publicly available information sources.

Box 4. Use of offshore service provider for the purpose of concealing financial flows

This example is based on fact patterns provided by Sweden and the United Kingdom

An offshore service provider was observed providing package services to its clients, which included anonymous offshore-prepaid cards and offshore structures, associated with offshore bank accounts. These services were all advertised online. The clients were encouraged to use encrypted email domain to communicate with the offshore service provider to ensure secrecy. The clients were able to use various methods to add credit to their offshore-prepaid cards including sending cash via a money service business and routing funds through various correspondent banks before reaching the offshore service provider's account. The offshore service provider held bank accounts with several different banks, which were frequently changed to avoid detection by law enforcement authorities.

1.2.3. Providing false documentation

15. Many countries reported that professional enablers provide false documentation as a key service to clients. Their professional knowledge is used to either produce false documents that appear genuine, or fraudulently alter genuine documents, which allows their clients to commit tax evasion supported by false or altered information. Whilst many legal and regulatory obligations such as requirements to provide annual tax returns, statutory accounts, or underlying source documentation for transactions for incorporated companies would normally act as barriers to the ability to commit tax crimes and other financial crimes, countries identified that professional enablers were providing false paperwork to either allow their clients to evade their tax responsibilities, or to provide organised criminals with an image of legitimacy and to dupe investors, suppliers, customers and investigators.

16. Another difficulty identified by several countries is that sometimes not all parties involved will be aware of or acting in concert with the professional enabler that has falsified or manipulated documents. This puts bona fide third party purchasers at risk of being deceived or defrauded. It is therefore all the more important to have sanction regimes targeting the professional enabler specifically.

Box 5. Falsified documents to evade taxation on income

A tax adviser sets up structures for a high net worth individual, Ms X, to help her evade paying taxes on her income. The tax adviser is known for marketing a specific tax evasion scheme, whereby he advises clients to emigrate from their home country to a foreign jurisdiction, but to deliberately stay shorter than the minimum amount of days required for them to establish tax residency in the foreign jurisdiction. The tax adviser then files an income tax return on Ms X's behalf in her home country, with falsified information and documents apparently showing that Ms X has emigrated and has no further personal connection with her home country. This creates the fiction of Ms X being a tax nomad who is then not taxed on her worldwide income either in her home country or in the foreign jurisdiction. In reality, Ms X continues her usual residence in her home country, and is able to evade taxes on her income through a legal fiction created by her tax adviser and his forging of documents for the tax authorities.

Box 6. Falsified documents to obtain an unjustified tax refund

This example is provided by the United States of America (IRS, 2020[6])*

Federal income tax returns are due to the Internal Revenue Service (IRS) annually. Many US citizens choose to pay an accountant or tax return preparer to prepare and file their federal income tax returns instead of preparing their tax returns themselves. The IRS authorises accountants and federal tax return preparers to enrol and become an authorised e-file provider. Unfortunately, a very small percentage of tax return preparers utilise their expertise for perpetrating fraud instead of assisting US citizens with legitimately preparing and filing their federal income tax returns.

In this example, the tax return preparer, unbeknownst to their clients, reported fake business losses and charitable contributions on their clients' federal income tax returns. The false information (manufactured business losses and charitable contributions) resulted in lowering a person's taxable income and thus increasing their federal tax refund. The clients of the return preparer became loyal customers because their federal tax refunds were generally higher than if they went to another return preparer.

The fraudulent information reported on the tax returns, for all clients over three filing periods, resulted in a tax due and owing for criminal purposes that exceeded USD 1 million. The tax return preparer was sentenced to 37 months in prison and will not be permitted to operate a tax business.

* Note: This example is provided through publicly available information sources.

1.2.4. Assisting in insolvency, bankruptcy and liquidation

17. Insolvency provides an opportunity for individuals who, assisted by professional enablers, can abuse the system to evade investigation and payment of tax and other debts. Insolvency related fraud occurs when a company is trading fraudulently and often takes place prior to the anticipated insolvency of the company. Although bankruptcy applies to the financial status of an individual, the victims are often the businesses that have provided the individual with credit, and the tax authority that is owed taxes.

18. "Phoenix company fraud" or "phoenixing" occurs when the assets of a failing company are transferred to a new company (the phoenix company). The failed company is then wound up, leaving a

trail of debts and out-of-pocket creditors, including tax authorities, behind it. The new company is often the same or similar to the former one but is able to trade with a clean record.

19. It is legal to form a new company from the remains of a failed company, but fraud happens when directors abuse the phoenix company arrangement by transferring the assets of the failing company below their market value, usually to another company beneficially owned by them or a related party, before insolvency. By doing this, the directors fraudulently reduce the funds available to creditors when the original company becomes insolvent.

20. Professional enablers may step in to create a company nominally controlled by a third party (which may or may not be fictitious), facilitating the creation of a beneficial ownership structure through which the controllers of failing companies can channel assets before liquidation. As a result, the creditors are left out of pocket, including the tax administration, which is a creditor for the outstanding tax liabilities. Some countries have legal provisions that allow liquidators or creditors to take action against those individuals personally who try to shelter behind the corporate veil of the company.

21. Below is an anonymised case of convicted phoenixing fraud.

Box 7. Phoenix company fraud

Mr X and his accomplice Mr Y ran a pre-appointment insolvency business. Mr Y created a fictitious identity – known as Mr Z – and provided those details to Mr X who used the fictitious Mr Z to:

- Lodge false and misleading documents appointing Mr Z as a company director;
- Replace a real person acting in the role of director with the fictitious identity, and backdating the director appointment by 18 months, and
- Create other false corporate records using the fictitious identity including taxation and employment records.

Mr X used the fictitious identity to facilitate deeds of company arrangement for debts owed by three companies in external administration. By creating the fictitious Mr Z, the professional enablers Mr X and Mr Y were able to claim that the new phoenix company was in Mr Z's control, even though it was effectively in the beneficial ownership of the failing companies' owners. This arrangement allowed the professional enablers to wrongfully strip assets from the failing companies to the fictitious Mr Z's company, before the failing companies were liquidated.

Mr Y and Mr X had previously provided pre-appointment insolvency advice to the directors of these companies and four other companies. The investigation was launched after a report of misconduct was received from an external liquidator of one of the failing companies.

1.2.5. Enabling tax fraud through cum-ex arrangements

22. An example illustrating the differences between legal and illegal practices carried out by professional enablers is the so-called "Cum-ex Files Scandal", which came to prominence in the mid-2010s. Tax advisors and lawyers have employed for decades a "tax-optimisation" strategy known as "dividend stripping", or "cum-cum", which consists of transferring stocks to a foreign entity to avoid paying dividend tax, and then re-selling them to the original owner. Dividend stripping is in the "grey area of the law"; moving stocks to a jurisdiction where dividends are not taxed right before the day when dividends are paid is not illegal in many countries.

23. When dividend stripping was prohibited in Germany, professional enablers devised a new strategy, known as "cum-ex". Cum-ex was an illegal tax fraud scheme that involved a sophisticated patchwork of

intermediaries and corporations that exchanged stocks multiple times for a very short period of time around dividend payment day. A stock is exchanged so many times and so quickly, that revenue agencies can no longer tell which owner paid taxes on the stock and which one did not, and ends up refunding taxes it never collected. The professional enablers devised this fraudulent tax scheme and actively marketed it to sophisticated clients, including several major banks, and implemented it knowing that it was a criminal offence under the laws of several jurisdictions. Cum-ex behaviour constitutes tax fraud in most jurisdictions, and as such is an illegal activity in which the professionals who enabled it have criminal liability. Therefore, these professional enablers deliberately avoided deploying the scheme in countries where they knew they would most likely be prosecuted.

24. While dividend stripping is not illegal under the laws of many European Union member states, it is a harmful practice that has cost EU member states over EUR 55 billion in unpaid taxes over the past 15 years, most notably Austria, Belgium, Denmark and Germany. The cum-ex fraud scheme cost the German government at least EUR 7.2 billion in lost revenue between 2005 and 2012.

25. The following is an example of dividend stripping and the fraudulent “cum-ex” tax arrangement.

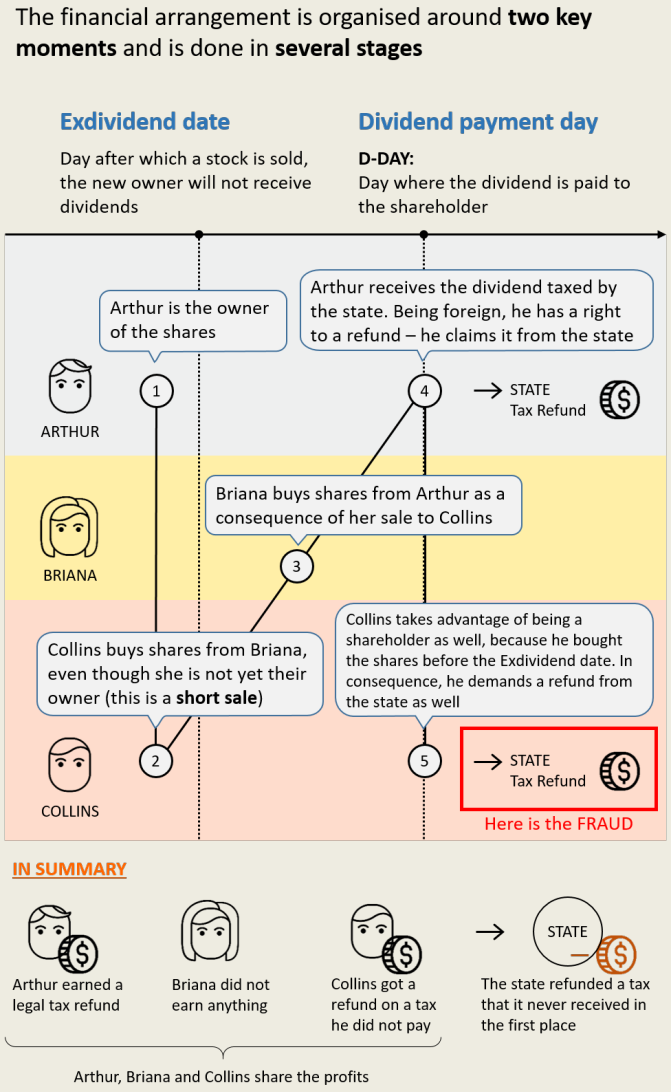
Box 8. Dividend stripping and “cum-ex” arrangements

Dividend stripping

Before dividends are paid, Andrew, shareholder of a French company resident in the United States, transfers his stocks to Boris, another shareholder based in Dubai. On the dividend payment date, the dividends are paid to Boris in Dubai. In accordance with the convention between France and the United Arab Emirates, dividends paid to Boris are not taxed. After the dividend payment date, Boris returns his shares to Andrew, together with the dividends earned. Thanks to this “dividend stripping” strategy, Andrew manages to avoid paying tax on his dividends.

Cum-ex

The illegal cum-ex scheme is more sophisticated than traditional dividend stripping strategies, as shown in the diagram below. In the diagram, the professional enablers Arthur, Briana and Collins work together, and will share the gains from this fraud.



Source: Agathe Dahyot/Le Monde, Nook Fulloptin & Alice Design/Noun Project

1.2.6. Enabling financial crime through crypto-assets

26. Virtual assets are a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes (FATF, 2012-2019[7]). This definition encompasses virtual assets that are both convertible and non-convertible to fiat currency (FATF, 2014, p. 4[8]). For the purposes of this report, the term "crypto-asset" refers to virtual assets in the form of tokens that are convertible to fiat currencies such as the US dollar or the euro (for example Bitcoin, Ethereum, Litecoin, etc.). The term "wallet" refers to crypto-asset accounts that can be used to store crypto-assets either online or offline. Furthermore, virtual asset service providers refers to natural or legal persons, who provide services, such as the exchange, transfer, safekeeping, or other participation in the provision of financial services (FATF, 2012-2019, p. 127[7]).

27. The risks posed by crypto-assets in enabling financial crime have been highlighted by the FATF since 2014 (FATF, 2014[8]) (2019[9]). However, the role of professional enablers in crypto-asset enabled financial criminality is not currently well documented and continues to evolve. It is possible that skilled

professional enablers, who engage in traditional models of financial criminality, may also utilise crypto-assets as part of their criminal schemes. As noted in the OECD's *Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors*, crypto-asset traders who agree to exchange crypto-assets face-to-face for fiat currency may play an important role in money laundering operations, with the potential to act as professional enablers (OECD, 2019[10]). The fact that crypto-assets are a type of tokenised virtual asset that often has lower levels of regulation and visibility by authorities than fiat currencies, which can allow for a higher degree of anonymity in transactions and obfuscation of financial flows, are all factors that make crypto-assets attractive to tax evaders and other criminals.

28. Professional enablers in the crypto-asset environment may also include operators of black marketplaces on the dark-web (e.g. the now-defunct Silk Road). These marketplaces enable criminals to buy and sell contraband, such as stolen goods, drugs, child pornography, weapons or other illegal items and services. Because the operation of these marketplaces requires a very high degree of technical expertise, the operators of these services can be characterised as professional enablers of criminal activities including, but not limited to, financial crime. The use of these marketplaces also necessitates technical expertise on the side of its customers to be able to access the marketplace on the dark-web with anonymity, which professional enablers may also facilitate. This means that professional enablers can also serve as intermediaries between the operators of the marketplace, sellers of illegal goods and services and the end customer who transacts through it. Dark-web marketplaces utilise crypto-assets as the primary payment method for their transactions in order to exploit enhanced anonymity and the ability to facilitate transactions that circumvent safeguards within the traditional regulated financial system.

29. Most crypto-assets based on a public blockchain (such as Bitcoin) operate with a high level of token flow transparency. All transactions are made available to the public through blockchain explorer services, allowing anyone to "follow the tokens" and audit any transactions occurring on the public blockchain. This means that when e.g. Bitcoins are stolen from an exchange, they become "tainted", because other users can track the origin of the proceeds. As a result, in order to conceal the tainted nature and traceability of the Bitcoins, stolen crypto-assets must first be laundered, before they can be withdrawn from the system (converted to other crypto-assets or to fiat currency).

30. Professional enablers may facilitate the laundering of proceeds of crime through the use of a crypto-asset mixing service (CMS).[3] A CMS is a paid service that has the potential to allow criminal actors to mix their criminally derived crypto-assets with legitimate crypto-assets of other users, in order to obscure the token trail and attempt to launder "tainted" crypto-assets through anonymisation.[4] After pooling the assets together, the CMS sends them back to its users, usually into newly-created wallets. This would allow criminals to obtain untainted crypto-assets in fresh wallets, making it extremely difficult to uncover their criminal origin. It is worth noting that there is no limit on the number of wallets a crypto-asset user can create. Furthermore, unlike with creating a user account on most crypto-asset exchanges, there are no customer due diligence requirements for a new wallet to enter the blockchain. Therefore, criminal actors can create and use thousands of wallets in order to obscure their transactions and activity on public blockchains.

31. A CMS can therefore make it easier for users to conduct criminal activity on the dark-web, as well as to launder proceeds stolen during for example a crypto-asset exchange attack. In this case, the professional enablers may be the companies that intentionally operate this service using their proprietary algorithms to facilitate money laundering, or other facilitators who manage the process of anonymising criminally derived assets through a CMS. As this is an emerging technology that may pose risks of financial crime and be a new avenue of activity by professional enablers, it is an area for countries to continue to

[3] These services are also known as crypto-asset tumblers, blenders or Bitcoin mixers.

[4] A "tainted" crypto-asset refers to tokens that can be linked to a specific transaction that indicates a crime (e.g. theft of crypto-assets from an exchange).

consider in terms of risk, supervision, and regulation. In recognition of the risk of financial crimes posed by virtual assets and virtual asset service providers, the FATF has revised its standards to recommend that countries should ensure that virtual asset service providers operating in their jurisdiction are able to manage and mitigate the risks of engaging in activities that involve the use of anonymity-enhancing technologies (FATF, 2019, p. 28[9]). A CMS is typically a virtual asset service provider within purview of the FATF standards, as they facilitate exchanges and transfers of virtual assets.

Box 9. Crypto-asset mixing service (CMS) case – Bestmixer.io seizure

Bestmixer.io was launched in 2018 and soon became one of the top three largest crypto-asset mixing services. By 2019, the company achieved a turnover of approximately 27 000 Bitcoins, worth roughly USD 200 million.

Since June 2018, the Dutch Fiscal Intelligence and Investigation Service (FIOD) has collaborated with the internet security company McAfee to investigate the service and determine whether it is laundering criminal proceeds.

The investigation has shown that many of the mixed crypto-assets on Bestmixer.io had a criminal origin or destination, meaning that the service was probably used to conceal and launder criminal proceeds. On May 22, 2019, six servers of Bestmixer.io were seized by the FIOD, EUROPOL and Luxembourg authorities. FIOD gathered information on all the interactions on the platform between 2018-2019, including IP addresses, transaction details, Bitcoin addresses and chat messages. This information is currently being analysed, in collaboration with EUROPOL.

On February 17, 2020, FIOD arrested a 31 year old man, suspected of laundering over EUR 100 000 with two accomplices. The arrest was made in connection with the investigation into Bestmixer.io. The suspect was discovered through his IP address, which was linked to a Bitcoin wallet that used the CMS to launder criminal proceeds. FIOD stated that more arrests are possible in connection with its investigation into Bestmixer.io.

As of 2020, there are numerous CMS operating in the crypto-asset environment, posing significant risk of money laundering using crypto-assets.

2 Identifying professional enablers

To be able to address the threats and risks posed by professional enablers, processes need to be in place to identify and capture relevant information about them.

2.1. Organisational awareness of professional enablers

32. Professional enablers are likely to be encountered across a number of different functions involved in a tax authority's compliance activity, from those business areas involved in promoting voluntary compliance, to those undertaking audits or investigations, through to those leading on enforcement activity such as civil penalties and criminal prosecution. If staff across the tax authority are not aware of what a professional enabler is, then it is likely that professional enabler threats may be missed.

33. Establishing and raising staff awareness is therefore crucial to improving the overall understanding of the threats and risks posed by professional enablers. In the United Kingdom for example, electronic learning packages have been created for tax authority staff to explain what is meant by the term 'professional enablers' and what to do if they identify one. Another approach is to designate a lead official in each organisation who is responsible for the issue of professional enablers. This person can serve as a key contact point for staff members to raise questions and share feedback on cases involving professional enablers. This person could also have responsibility for raising awareness in the organisation through briefings, meetings and training sessions, and serve as a member of a broader national team responsible for implementing the professional enabler strategy.

2.2. Measuring the threat of professional enablers

34. Once a country has defined the parameters of its professional enabler definition, it can consider how to identify, record and measure professional enabler activity. Measuring the threats and risks posed by professional enablers is important, as understanding the size and nature of the problem will then help to determine the best approach to addressing it.

35. Not all countries have taken the same approach to tackling professional enabler issues. Some countries have chosen to focus resources on specific types of professional enablers or professional enablers in higher risk sectors, with multiple and concurrent strategies depending on the area of focus. Therefore, the appropriate measure will depend on the scope and objectives of a country's professional enabler strategy.

36. Measuring the size and nature of the professional enabler issue will involve identifying all the potential data sources, which may contain references to enablers or their clients, and then developing methods for detecting the risks that they pose. This may involve identifying indicators within existing data such as suspicious patterns of behaviour in a sector that may indicate enabling of tax crime, or creating new indicators such as the capture of internal management information to show when a professional enabler is being investigated. For example, in the United Kingdom, internal information management systems now allow staff members involved in open investigations to indicate if a professional enabler is

suspected of involvement in a case or not. This information is collected and recorded in one place, which allows the authorities to have a single overview of enabler cases. The type of measures and indicators for each country will naturally depend on the type of data available, and may require multiple strategies for different risk areas. Creating this baseline of understanding is important, as it will provide the foundation for measuring the success of any subsequent strategy for tackling professional enablers.

2.3. Detection through development and analysis of professional enabler indicators

37. Use of data and intelligence is an essential tool to help identify specific professional enablers, as well as the broader pattern of schemes and structures they use. However, because professional enablers are a sub-set of professionals, operating in a range of transactions that may be overseen by different regulatory or investigative bodies (e.g. professional regulatory bodies, financial regulators, financial intelligence units, and tax administration), intelligence is often held in different databases and systems both within and across organisations. This makes it difficult to identify trends and patterns or even repeat offenders. Improved risk analysis of individual professional enablers is one way in which to grow the pipeline of investigations and interventions, and build up effective coordinated disruption and deterrence efforts.

38. Many countries have dedicated teams focused on compliance work specifically relating to a known problem area, such as targeting enablers that are associated with multiple shell companies or that market the use of offshore structures. For example, many countries have collected information on professional enablers connected to offshore service providers or firms for the purpose of utilising it in data analytics and audit strategies. Feedback from countries show that offshore jurisdictions known as “hotspots” of activity for specific evasion structures are often utilised repeatedly by the same professional enablers. Once a particular structure or nefarious service provider is uncovered, this gives tax authorities the ability to target other structures established by the same professional enablers. However, feedback from countries also shows that these hotspots can fluctuate, for example in response to detection or where a new strategy is devised, and therefore national professional enabler strategies need to be flexible to adapt to new information and intelligence received. Box 10 highlights some of the indicators identified from case studies from TFTC countries, which could be used for risk assessment exercises. Box 11 is an anonymised case study of a scoring model system developed to identify professional enablers through specific professional services targeted by Country X.

Box 10. Possible indicators for use in risk assessment exercises for detecting involvement of professional enablers

- A company is not found at the declared premises
- Addresses of entities or directors which are not traceable
- Multiple shell companies from the same address
- Multiple companies with directors in common
- Company’s address registered at a P.O. Box address known for illegitimate businesses
- Professionals with a high turnover of business relating to liquidation of small companies
- Professionals that promote tax schemes on the basis of premium or contingent fees, or contractual protection that guarantees coverage of any financial liabilities resulting from the tax strategy

- Where one individual is attributed as a director multiple times, the extent to which the provision of substantial and meaningful directorship services could not be feasible
- Tax intermediaries with poor tax compliance and filing history
- Persons with association to known professional enablers
- Persons with association to known tax evasion structures
- Persons with association to known offshore structures that obscure beneficial ownership to facilitate fraudulent behaviour

Box 11. Scoring model to identify professional enablers in Country X

The country providing this case study has requested to remain anonymous

Country X does not have a defined class of professional enablers that it targets in its strategy. Instead, Country X's methodology utilises a scoring model to find professional enablers who offer tax evasion products with a cross-border element aimed at evading taxation in Country X or rendering detection of tax evasion difficult for the authorities (based on an assumption that these professional enablers advertise their products). The methodology uses the tax authority's own internal systems and also internet searches to locate offerings of such professional advisory services with a correlation to Country X. The searches are conducted based on 60+ keywords to detect these specific professional services, with a scoring model that assigns different weighting for countries, behaviour patterns, and trigger words, on a risk basis. This scoring model is therefore able to yield Country X a risk-weighted result of service firms and professional enablers to focus on for investigation.

Subsequent investigations can include analysing money transfer data to and from particular service providers or enablers identified through the above scoring model. This allows Country X's authorities to garner a picture of the type and breadth of clients utilising the enabler's services, and identify patterns and trends. It also informs further investigations on the individual clients, enablers, and firms involved.

2.4. Data sources for identifying professional enabler activity

39. The following methods listed in the box below were highlighted by countries as useful in identifying wrongdoing by professional enablers.

Box 12. Data sources in professional enabler investigations

- Data mining information from offshore leaks, looking for links to professionals active in the jurisdiction, common clients of those professionals, and common structures
- Analysing information from suspicious transaction reports (STRs), including STRs on international electronic funds transfers, to identify repeat transactions, professions or persons that are the subject of the reports
- Creating a reporting mechanism for officials across the tax administration to report suspicions or queries with respect to intermediaries that are involved in suspect structures or transactions
- Information from voluntary disclosure programmes

- Anonymous or whistle blower reports
- Information on the internet advertising tax schemes or offshore structures
- Statistics on companies that have been struck off and cross-matching that information to companies served by the same service provider
- Statistics on disqualified directors and cross-matching that information to those that work for the same service provider
- Creating an internal database of shell companies, suspicious addresses, suspicious directors and persons etc. to query or use for data mining
- Creating a database of known professional enablers and known associates
- Validating the authenticity of documents with relevant government agencies (e.g. passport office, company registrar, financial regulators, other law enforcement authorities etc.)
- Validating the identity of taxpayers through signatures, photos or fingerprints in tax authority or government records
- Consulting the OECD ATP Directory, a confidential database of over 400 aggressive tax planning schemes (OECD, n.d.[11])

40. An example from India of how data mining was used to find fraudulent taxpayers, directors and other professional enablers is included below.

Box 13. India's use of data sources in professional enabler investigations

In 2017, the government of India set up a special task force dedicated to the identification and eradication of shell companies. Shell companies are recognised as a risk to the tax base due to their usage in the commission of tax crimes and other financial crimes.

As a country with a large population, information in India on individuals, taxpayers, corporations and directors are held in different databases by separate government departments and ministries. Information on individuals is maintained by the Unique Identification Authority using "Aadhaar" numbers, a biometric-based unique identification number for individuals. Information on taxpayers is held by the Income Tax Department through permanent account numbers (PANs), a unique taxpayer identity number that is mandatory for all taxpayers (but not necessarily all individuals). Finally, the Ministry of Corporate Affairs manages the register for corporate entities and directors through the registering of corporate identity numbers (CINs) and director identification numbers (DINs).

One of the key tasks in identifying shell companies was to be able to perform data analytics across the information held by the three different government departments and data-mine between the three databases. The results of this triangulation of information between government departments were dramatic. By linking the information between Aadhaar numbers and PANs, many ghost PAN holders, duplicate PAN holders or fake PANs were identified and removed from the system. Cases of fraudulent non-quoting of PANs were also identified, which was previously a common way for fraudsters to remain undetected by the Income Tax Department, leading to high value transactions being concealed and fraudsters escaping investigation or audit. The crosschecking of information with DINs and CINs also revealed the identify of fraudulent directors and shell companies. This was evident when anomalies were found for companies that had filed financial statements but failed to file an annual tax return, or vice versa, where companies had filed an annual tax return but failed to file financial statements, as required. This resulted in the disqualification of 309 000 directors, and 226 000 companies being struck-off by the Ministry. Furthermore, in the process of this crackdown on fraudulent activity by directors,

fraudulent PANs and companies, approximately 400 professional enablers were identified as responsible.

This straightforward action of combining information and databases that were already in the Indian government's possession, was able to root out thousands of cases of basic fraud and non-compliance by individuals, companies, directors and other professional enablers such as accountants. In particular, the triangulated information also gave the Indian authorities a clearer picture of where wrongdoing was being perpetrated by the same sets of persons repeatedly, which indicated where professional enablers might be involved and further investigation would be warranted.

3 Disrupting professional enablers

Lawyers, tax advisors, notaries and accountants are valued gatekeepers to a sound legal and financial system. Their unique sets of skills, together with the professional privileges awarded to them by statutes, put them in a special place within societies. They are experts who are in a position of trust, and enjoy certain rights that are not shared by other professions. Jurisdictions should ensure that advisors perform their tasks in accordance with the law, and penalise those few who use their skills, expertise and privileges to design structures with the purpose of breaking the law. This requires that countries have in place a legal framework to support criminal investigators and the justice system in addressing and punishing professional enablers that engage in and facilitate the commission of such crimes.

41. For the most grievous offenders, it is important that countries have in place criminal sanctions for professional enablers to penalise them for their wrongdoing. Countries have also reported the use of civil penalties, injunction mechanisms or disbarment through professional supervisory and regulatory bodies as secondary and tertiary methods for authorities to disrupt, deter and penalise offenders, which may be more appropriate in reflecting the different types of involvement of professional enablers. Ensuring that a cascading range of legal sanctions and disruption tools are available to government authorities allows law enforcement agencies to have the flexibility and framework to address the risks posed by professional enablers.

3.1. Legal sanctions for professional enablers

Countries have reported a variety of legal approaches to sanctioning the actions of professional enablers. Jurisdictions should address the issue of criminalising the conduct of professional enablers in accordance with their domestic legal frameworks. In general, countries do not separately criminalise professional enabler behaviour, but address it through provisions criminalising accessories to tax crime, or as an aggravated accessory offence where an enabler is involved in a tax crime. Some countries also have civil penalty regimes that specifically target professional enablers and promoters.

42. Professional enablers represent a distinct type of secondary offenders, whose actions can be criminalised by being defined as the aiding, abetting, facilitating or enabling of a tax offence. Professional enablers can also be treated by some countries as special accessory offenders with regard to tax crimes and other financial crimes, who are liable to a higher penalty than regular aiders or abettors.

43. Some countries have reported that such accessory offence provisions have been well utilised to prosecute the actions of professional enablers in the commission of a tax crime or other financial crimes. In other countries, authorities have experienced difficulties in using accessory criminal offences against enablers due to lack of precedent, high levels of administrative burden to prove the offence, or inability to successfully prosecute the primary offence. Some countries, such as Australia, France, and the United Kingdom, also have significant civil penalty provisions that target professional enablers or promoters of tax

evasion schemes, and an example of the administrative sanctions for facilitators in France can be found in Box 14 below.

Box 14. Administrative sanctions against facilitators in France

Law No. 2018-898, of 23 October 2018, introduced a new tax fine for intermediaries who are facilitators of serious breaches by taxpayers. A new administrative sanction was also introduced; separate from criminal sentencing, which is applicable to persons who, through their services, contribute to the preparation of fraudulent or abusive arrangements.

The law sets the list of services that can be punished, including:

- Allowing the taxpayer to conceal his or her identity by providing a fictitious identity or a nominee or by using a natural or legal person or any foreign-based organisation, trust or comparable institution;
- Allowing the taxpayer to conceal his or her situation or activity by a fictitious act or by the intervention of a fictitious entity;
- Allowing the taxpayer to wrongly benefit from an income deduction, a tax credit, a tax reduction or an exemption from tax by the improper issuance of documents;
- Carrying out on behalf of the taxpayer any action intended to mislead the administration.

The amount of the fine is set at 50% of the income derived from the service provided to the taxpayer, but may not be less than EUR 10 000.

44. Where countries are considering introducing specific criminal law provisions to address professional enablers, key elements to be considered could include:

- Defining professional enablers as accessory offenders to tax and economic crimes in accordance with the technical features of each national legal framework;
- Enactment of legislation that specifically targets and penalises enablers of tax crimes and other financial crimes;
- Extending sanctions beyond imprisonment and fines (e.g. disqualification) and applying different types of sanctions according to the different levels of intent;
- Lifting professional privilege in regards to privileged evidence of professional enablers when being directly investigated for the commission of a tax or economic crime;
- Setting appropriately lengthy statutes of limitations and grounds for its interruption and suspension that acknowledge the time-consuming and complex nature of these types of investigations;
- Ensuring there is a legal basis for co-operation of professional oversight bodies with investigators;
- Ensuring investigative agencies have adequate legal tools for engaging in complex investigations regarding professional enablers (e.g. powers to seize evidence and assets, and to interview witnesses and suspects).

Box 15. Legal reforms in Mexico to tackle professional enablers

Mexico has introduced multiple legal reforms in recent years to combat the increasing prevalence of professional enablers and their vast networks and operations in Mexico.

These legislative reforms included amending federal laws to formally include tax crimes in the catalogue of organised crime offenses, which were specifically intended to encompass and target the activities of

professional enablers. The prosecution of professional enablers under the Organised Crime Law carries a sentence of up to 16 years imprisonment, in addition to any penalties applicable for the prosecution of the underlying tax crime. Furthermore, the legislative powers under the Organised Crime Law allows for the confiscation of assets relating to organised crime offences even where there is not yet a verdict in a criminal trial, as a pre-emptive step to discontinue the activities of the professional enabler and ensure that assets that give rise to or are a product of tax crime are adequately secured.

The reforms expanded the application of the United Nations Convention against Transnational Organized Crime to tax crimes under Mexican national law, allowing Mexican authorities to have further recourse to special investigation techniques such as undercover operations, witness protection measures, and the intervention of private communications, including in cases of crimes facilitated by professional enablers.

Furthermore, the Law of National Security was amended to add certain aggravated tax crimes to the catalogue of acts against national security, for example where falsification of documentation is facilitated by a professional enabler. This legislation allows the Mexican courts to order imprisonment as a preventive measure to those accused of partaking in an aggravated tax crime as a professional enabler, and enhances resources available to the Mexican Fiscal Prosecutor in such cases.

Finally, the Federal Criminal Code has been amended to extend the application of criminal responsibility for the majority of tax crimes to corporate entities as well, to ensure that entities that enable tax crimes are caught within the net of the Criminal Code.

The suite of legislative reforms enacted by Mexico reflect the seriousness of this issue for the Mexican government, and the necessity for authorities to have the appropriate powers enshrined in legislation in order to investigate, prosecute, sanction and deter the activities of professional enablers in their country.

45. It is important that sanctions against professional enablers of tax crimes and other financial crimes have a deterrent effect. One important aspect of deterrence is having in place strong penalties. Penalties should be sufficiently dissuasive, whether monetary fines, confiscation of assets or imprisonment, such that professionals would be deterred in practice from engaging in enabling behaviour.

46. As aforementioned, criminal sanctions should be applied to the most egregious of professional enabler offences, to underscore to the public that those who commit serious tax crimes face serious consequences, in recognition of the harm to society that the actions of such professional enablers cause. For such cases, these professional enablers should be publicly and openly prosecuted to have the appropriate reputational and deterrent effects in society, and promote a strong culture of tax compliance and tax morale. An example of a successful criminal prosecution of professional enablers in France is provided below in Box 16. It will be up to each country to decide on whether criminal prosecution or civil sanctions provide the best approach, and these options should form part of a country's strategy for dealing with professional enablers.

Box 16. Investigation and prosecution of professional enablers in France

In October 2008, a specialised inspection squad of the French tax administration organised a raid at the business premises of a company service provider, suspected of facilitating tax fraud. The search disclosed a vast scheme allowing French clients to avoid paying their taxes and launder money, uncovering evidence for both tax and financial offences. The documents discovered revealed that the French businessperson contacted hundreds of French clients to sell ready-made shell companies incorporated in financial centres or non-European low tax jurisdictions.

The evidence showed that the suspected French businessperson, who once promised "tax haven for all", had helped tax evasion to become easier and cheaper among ordinary taxpayers and small businesses in France.

The French Office of the Public Prosecutor began a criminal investigation into this matter in July 2011. The investigative results showed that the business was staffed by two French lawyers, a foreign director and nominee shareholder, as well as support staff located in Paris and abroad. The tax evasion schemes utilised foreign banks, which provided private bank accounts and credit cards to the French clients, especially one European bank in the Baltic area. The criminal investigations also identified that the perpetrators organized "large-scale" tax evasion through a network of offshore companies, in connection with offshore company service providers as well. The true beneficial owners of the shell companies were not revealed to the local company registry. Furthermore, the French professional enabler himself evaded tax on his own earnings through the same offshore tax evasion schemes.

In addition to the professional enablers of this fraud, customers that utilised the tax schemes also became the subject of tax proceedings. The French tax administration led tax audits on all the clients identified by the investigations.

The French criminal court sentenced the French organiser of this vast scheme and his accomplices as follows:

- The main perpetrator was found guilty of tax fraud, forgery of documents, fraud, money laundering and criminal association. He received a jail sentence, five years imprisonment with two years probation and a fine of EUR 3 000 000. He was also prohibited to conduct any further business and management consultancy activities.
- One of the French lawyers who assisted in the operations of the schemes was convicted of aggravated money laundering and was sentenced to three years suspended imprisonment and a penalty of EUR 50 000.
- One of the banks involved was found guilty of money laundering and was sentenced to a fine of EUR 80 000 000, and prohibited from conducting business in France for five years.

The coordinated action between the French tax administration, criminal investigation and prosecution services was able to successfully investigate, prosecute and sanction the French professional enabler and his accomplices. This case was openly prosecuted and highly publicised in the media. The criminal sanctions applied were effective to disrupt the illicit activities of the enablers, and underscore to the public that serious penalties apply for professional enablers of tax fraud and money laundering, to both individuals and financial institutions alike.

47. In practice, lower level cases of professional enablers may require different approaches for a number of reasons: there may be administrative reasons such as limited resources available for authorities to prosecute only the most serious of professional enabler crimes, or the nature of involvement by the professional may not warrant a criminal or civil sanction. The following sections therefore look at other methods available to authorities to disrupt the actions of professional enablers.

3.2. Injunctions

Court orders and injunctions against practicing law, accounting or advisory services have been cited as tools that countries can use to disrupt professional enabler's behaviour. Depending on the country and the profession involved, injunctions can be used to require, or restrain an enabler from, specific behaviour upon

application to the courts, or can be used to remove professional enablers from operating in their area of expertise all together.

48. For example, in the United States, fraudulent tax return preparers and tax-fraud promoters can be addressed through both civil and criminal enforcement tools. A civil injunction program, administered by the United States Department of Justice Tax Division, can bar individuals or businesses from engaging in specified misconduct or from preparing tax returns for others. Any individuals or businesses found in breach of the injunction can have further criminal action taken against them. Furthermore, any fraudulent individuals or businesses that have been shut down by the Department of Justice (DOJ) via an injunction are listed publicly on the DOJ's website ([12]) ([13]). This makes all taxpayers and tax professionals aware of the identity of unscrupulous tax preparers and businesses, makes it clear that professionals who facilitate illegal conduct will be stopped, and acts as a deterrent in the industry to increase tax morale and a positive compliance culture.

3.3. Professional supervision and regulation

Most countries have regulatory and supervisory bodies for AML and CFT purposes, and professional bodies that self-govern their members through a code of conduct or similar set of ethical obligations. This could include for example, a bar association or law society for lawyers, or a chartered accountancy or international ethics and standards board for accountants (IESBA, n.d.[14]). These regulatory and professional bodies may receive reports of misconduct or criminal behaviour on the part of members of the profession, and may have the ability to impose sanctions and suspend or remove licences for businesses to legally trade, or the ability to expel members or firms from membership in the professional association. These bodies should be part of the strategy for addressing the behaviour of professional enablers.

49. A country's strategy and legal framework for professional enablers should therefore include co-operation with and the usage of regulatory and professional bodies or other supervisory bodies to ensure disbarment or disqualification of enablers where there is misconduct, so that these enablers can no longer continue their harmful services.

3.3.1. Supervision and regulation

50. Countries should have a robust supervisory and regulatory framework that puts in place the relevant FATF standards for anti-money laundering and counter-financing of terrorism. In particular, the FATF standards require the regulation and supervision of designated non-financial businesses and professions (DNFBPs) which includes lawyers, notaries, accountants, other independent legal professionals and trust and company service providers. The FATF has also produced guidance to support effective risk based supervision of the sector.[5] Having in place appropriate regulation and supervision of these sectors is important as it can have a deterrent and awareness-raising effect for enablers, whilst regular supervision will help countries to monitor and enforce the AML and CTF obligations for professionals and understand any ongoing and evolving enabler risks through continued dialogue with each sector. Such regulatory frameworks also allow for easier reporting and detection of suspicious enabler activity.

[5] See Annex A of this report.

3.3.2. Sanctions through regulatory or professional bodies

51. Supervisory and regulatory bodies may also have the ability to impose sanctions or suspend and remove licences of businesses or professionals that do not meet AML and CTF standards, and can be an additional tool in disrupting professional enablers of tax crime. An example provided by the United Kingdom is the use of supervision requirements under anti-money laundering and counter-terrorism financing rules to remove professionals in money service businesses or trust and company service providers that are not of a "fit and proper" status. This has been a quick and effective way to remove the ability of the business to legally trade, and stop professional enablers in their tracks, to limit criminal activity and further losses to tax revenue. Some countries utilise sector supervisors or professional boards to administer sanctions and regulate offences, as those bodies can hold an individual accountable to civil rather than criminal standards. These investigations can result in business closures and suspension or loss of licenses. While this means the subject will not be incarcerated, it does prevent the professional enabler from continuing to commit crimes by abusing his/her professional licence.

52. Using professional and supervisory boards also allows for greater publicity within a professional enabler's sector if the enabler's conduct and punishments are published in the profession's journal, on their website, or membership list. The following case study from India highlights the new administrative body it has put in place to strengthen the independence of oversight and the ability to execute professional disciplinary action.

Box 17. India's Task Force on Shell Companies

In 2017, the government of India set up a special task force dedicated to the identification and eradication of shell companies. As outlined in the case study contained in Box 13, India, using available data, was in the process of a crackdown on fraudulent activity by directors and fraudulent companies, whereby approximately 400 professional enablers were identified as responsible.

The list of 400 professional enablers was then shared with the Institute of Chartered Accountants of India (ICAI), for disciplinary action of its members. However, due to conflicts of interest with members of the ICAI, disciplinary proceedings stalled and never proceeded. The ICAI was a previously self-regulating professional accounting body. A new oversight body for the accounting and audit professions was legislatively provided for by parliament in 2013, but was not properly implemented until the recent creation of the National Financial Reporting Authority (NFRA) under the auspices of the 2013 legislation. The NFRA is charged with powers to investigate matters of professional misconduct by chartered accountants or chartered accountancy firms, with the ability to impose penalties, and debar the chartered accountant or firm for up to 10 years. As an independent regulator, the NFRA is now able to properly review the conduct of the professional enablers identified by the Task Force on Shell Companies, and take appropriate disciplinary action or debar accountants found to be guilty of misconduct.

3.3.3. Disqualification of company directors

53. Most countries reported having some form of disqualification process for directors of companies suspected of enabling crime. The process varies in each country, but the government authority responsible for governing corporate entities typically has the power and mechanisms for removal and disqualification of directors. The reasons prescribed for disqualification can differ, but the most common reason for disqualification is where directors fail to act at a time when they should have done so, whether it be filing for insolvency or taking action that will mitigate the losses of their companies, etc. The consequences of disqualification and the time period in which a person is barred from acting as a director vary widely

between jurisdictions. In some jurisdictions,[6] for serious offences, a disqualified director is barred from acting as a director forever.

54. Some jurisdictions also have public registers that list disqualified directors and are easily accessible. This has been noted as a useful tool for government authorities, as the disqualification of a director in one country does not prevent the same individual from acting as a director in another country. Public registers of disqualified directors, and increased sharing of intelligence among government authorities, allows authorities the ability to identify collectively any directors that are fraudulent professional enablers operating in multiple jurisdictions.

55. Although rules on company directors can vary significantly between jurisdictions, the following are some common safeguards that can be put in place by countries with regard to company directorships:

- Require that the director be resident in the jurisdiction. This can improve access to an accountable person in case of investigations, and also be a significant disruptive factor for criminals seeking to distance themselves from the crime.
- Require that directors pass a “fit and proper” test or equivalent threshold. This could include being subject to credit checks, and requirements to disclose previous directorships, any disqualifications both in the jurisdiction and abroad, any outstanding court judgments or criminal convictions, etc.

[6] For example Australia, India and the United Kingdom.

4 Deterring professional enablers

Targeting the actions of intermediaries before they become professional enablers can help to swiftly prevent growth of professional enabler risks, and communication and education can be key. Once professional enabler activity is occurring, mechanisms to deter and intercept it are necessary, such as leveraging the role of professional bodies and regulators, as well as creating mechanisms for voluntary or mandatory reporting and whistleblowing. This chapter describes the range of mechanisms countries can consider as part of their disruption strategy.

4.1. Preventing abuse

Professional enablers can be deterred from criminal activity through a number of methods, and an effective prevention strategy is generally more efficient than investigation in many cases. Countries use a range of communication, engagement and education, corporate responsibility and governance approaches to ensure would-be professional enablers are aware of the risk the misuse of their services can entail, and promote a culture of voluntary compliance.

4.1.1. Communication

56. A key prevention strategy is to provide clear and accessible guidance on the operation of the tax and criminal laws. Some countries also have dedicated teams to look at deterrence through communication activities, and develop strategies to create a culture of voluntary compliance. Communication should take place throughout the life cycle of a particular risk posed by professional enablers: before the professional enabler decides to pursue the activity; once a particular scheme is known; and after the successful prosecution of a professional enabler.

Before the professional enabler decides to pursue the activity: pre-emptive action

57. Pre-emptive communication strategies can include clear communication and guidance on the parameters of tax rules and consequences for non-compliance, regular engagement with tax professionals and taxpayers, helpful reminders of filing requirements, etc. These communication strategies can all promote a higher compliance culture and reduce opportunities for “grey areas” to be exploited.

58. Examples of pre-decision communications tools include:

- Online information through government websites: this can include publishing factsheets, guidance, public rulings, media releases, news articles and alerts
- Targeted emails to registered businesses, filtered by sector and location: for example, in the United Kingdom, a “welcome” email is sent to all newly registered businesses with links to relevant web pages and information to promote tax compliant behaviour

- Face-to-face events: regular engagement through presentations or dialogue with businesses, peak industry bodies, intermediaries and tax professionals, etc.
- Webinars: online, live presentations where tax professionals can take part in a live, interactive online workshop to raise greater awareness of their responsibilities and have the opportunity to ask questions. These have proved popular in some countries, especially with businesses in particular sectors where common questions can be addressed, and is a cost effective way to reach a large audience
- Regular podcasts to communicate to tax professionals new messages, concerns, or services provided by the tax authority
- Joint campaigns: working with other government departments and law enforcement agencies to help businesses understand their responsibilities
- YouTube video clips to educate customers and registered businesses including visuals. The aim is to support customers with regard to key services such as income tax or information technology registration to make voluntary compliance easier and more accessible.

Once a particular scheme is known: targeted action

59. Once a specific risk is known, targeted communication tools can also be used, such as communicating requirements under the law to boost compliance in areas with low levels of compliance or in areas of emerging risk. In the following, Box 18 is an example showing the Australian Taxation Office's usage of taxpayer alerts to warn taxpayers and tax advisers of emerging high-risk arrangements that the Australian Taxation Office is concerned about, and Box 19 contains an example from the United Kingdom's Her Majesty's Revenue and Customs approach to encouraging compliance in response to a known risk.

Box 18. The Australian Taxation Office – usage of taxpayer alerts to address new tax schemes

This example is provided by Australia

The Australian Taxation Office (ATO) publishes taxpayer alerts regarding new or emerging high-risk tax schemes. Where intelligence is received by the ATO of a risky arrangement that may not be compliant with the law, the ATO is able to respond with immediacy to warn the community. Through taxpayer alerts, the ATO is able to share with tax practitioners and taxpayers its concerns regarding an arrangement that is legally ineffective, involves exploitation or a deliberate misapplication of the law, or which may constitute tax evasion or tax fraud. Furthermore, the ATO can indicate what the applicable penalties are for taxpayers who use the tax scheme, or enablers who promote usage of the tax scheme.

The ATO's experience shows that the practice of using taxpayer alerts has the effect of preventing uptake of illegal tax schemes and preventing proliferation of a tax scheme's usage by further providers. In general, fewer mass-marketed schemes have been observed in this climate as a result.

Box 19. HMRC's "Promote and prevent" approach to encouraging compliance

This example is provided by the United Kingdom

HMRC has a number of "promote and prevent" approaches where, in addition to responding to identified risks, it proactively promotes compliance in specific customer groups or business sectors where those risks have occurred, in order to prevent future non-compliance.

- One-too-many approach: one message is sent to a wide audience (individuals and businesses) about a specific issue relevant to their type of business/tax responsibilities.
- Nudge: broad messaging to try to encourage a change in behaviour. This might be a change in the way a form is worded to encourage greater compliance, for example "Please can you do this" versus "You have to do this" versus "If you don't do this then the consequences will be this".

After the successful prosecution of a professional enabler: publicising outcomes

60. Finally, an effective deterrent measure is to publicise thoroughly all high-profile tax crimes committed, the enablers involved, and the punishments that criminals receive such as incarceration, penalties, and loss of license or business. This is important to underscore to the public that individuals who commit tax crimes face consequences, and reinforces fair taxation principles and the public's trust in the tax system, thereby contributing to higher tax morale (OECD, 2019[15]). It is common that countries do not disclose information about allegations and ongoing investigations until the case has been completed. However, upon case completion, there often is some form of publication about the criminal acts and the consequences of the offender's criminal behaviour. These successful prosecutions can be publicised via press releases by the law enforcement agency, along with appropriate communication strategies to ensure media coverage by other news sources, blogs, and professional journals. Making the public aware of the consequences of these behaviours is crucial to deterring similar actions in the future.

4.1.2. Engagement and awareness raising

61. Tax administrations can tackle non-compliant behaviour through engaging directly with professions that may be vulnerable to being professional enablers. By working with these sectors and their industry representative bodies, countries can develop a greater understanding about the business practices involved and deliver targeted education. This increased visibility for authorities can also allow countries to develop bespoke strategies to target high-risk enabler sectors if need be. In the prevention stage, where possible, this education is most effective when productive working relationships are fostered between taxpayers, their intermediaries, and tax administration colleagues.

62. Awareness raising activities in high-risk professional enabler sectors has produced positive results in some countries. Through industry engagement, consultative and educational activities, professional enablers who are less cognisant of their part in facilitating wrongdoing are made more aware regarding their role and the risk of their behaviour having legal ramifications. Furthermore, the raised awareness of the tax authority's scrutiny into an industry sector will typically have a deterrent effect, whilst giving government authorities greater visibility into the professional services industry behaviour and norms.

4.1.3. Promoting corporate responsibility and good governance

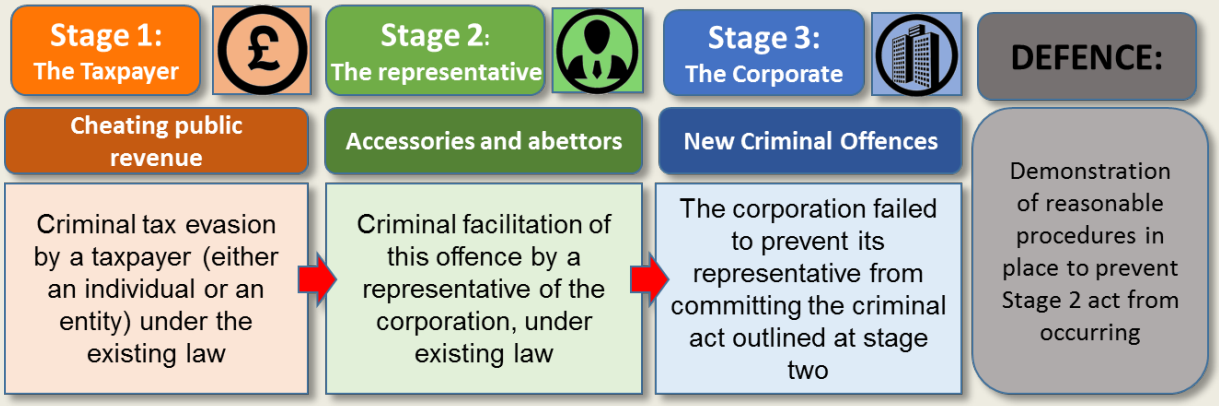
63. Professional enablers commonly provide services for or on behalf of a corporation. Here, the role of professional enablers can be shaped by the corporate culture of the organisations they work for and a

company's attitude towards tax compliance can directly affect the behaviour of a professional enabler providing services on behalf of that company. For example, behaviour may be influenced by direct incentives such as bonus systems that encourage risk-taking, deficiencies in systems such as employee training, or a culture that turns a blind eye to certain practices such as poor know-your-customer practices, or a lack of clarity from top-level management on refusing to engage in tax fraud. This is an issue identified in the United Kingdom, which has legislated to attribute liability to companies that have not prevented facilitation of tax crime within their organisations, as illustrated in the below example.

Box 20. The United Kingdom's legislation creating corporate responsibility to prevent criminal facilitation of tax crime

In the United Kingdom, for those professional enablers who provide services for or on behalf of a corporation, issues were identified in its law enforcement's capability to tackle the corporation's role in the facilitation of tax fraud. Attributing criminal liability to the corporation meant establishing proof that its senior members were involved in and aware of the illegal activity. This made it difficult to hold large multinational organisations to account (given their structures) and may have driven poor behaviours i.e. senior members of an organisation ignoring criminal acts committed by its representatives in order to protect their organisation from criminal liability.

Recognising this as an issue, the United Kingdom introduced new legislation in 2017 which holds those corporates to account which fail to prevent its associated persons (i.e. professional enablers) from criminally facilitating tax crime, referred to as the Corporate Criminal Offences (CCO). These offences seek to address the issues of attributing criminal liability to legal persons and places the responsibility on the corporate to take responsibility for improving its systems, controls and culture. The offences do not alter what is criminal at the individual level, but rather allows the corporation to be liable for failing to prevent an individual from committing acts that were already criminal.



CCO is a strict liability offence, meaning that if a tax crime has been committed (stage 1) and that fraud has been criminally facilitated by an enabler (stage 2) then the corporate would be liable under the new corporate offences, unless it can demonstrate that it has put in place reasonable procedures to prevent the facilitation of tax evasion by persons providing services for or on its behalf. This is the in-built defence of the offences and is designed to encourage corporates to take responsibility for putting in place systems and controls to prevent their representatives from facilitating tax evasion.

64. A country's professional enabler strategy should look to incentivise corporations to take responsibility for the behaviour of their organisation as a whole, including their representatives, and put in place appropriate systems and controls. Promoting a culture of good governance and corporate

responsibility is essential to support the public perception of the rule of law applying to large corporations. This is important to maintain trust in the tax system and have a strong culture of tax compliance and tax morale in a country. Maintaining a socially responsible corporate image is important to most businesses for reputational reasons, which in turn affects profits. Therefore, this ought to encourage corporates to be selective in the tax professionals and intermediaries they hire to ensure there is no association with recalcitrant professional enablers.

4.2. Disclosure facilities

4.2.1. Voluntary disclosure programmes

65. Voluntary disclosure programmes give taxpayers an opportunity to submit to tax authorities details of any previously fraudulent behaviour they have committed, such as not appropriately declaring income, inappropriately claiming deductions, credits or benefits, or falsehoods or omitted information from previous tax returns. Taxpayers are typically incentivised to make voluntary disclosures through such programmes due to offers of leniency or discounts on penalties and tax liabilities where a taxpayer makes a voluntary disclosure, or if they know that tax authorities will likely be made aware of their fraudulent tax affairs through transparency and exchange of information measures, such as the Standard for Automatic Exchange of Financial Account Information in Tax Matters (the AEOI standard). Voluntary disclosure programmes can operate indefinitely or for a limited time, and can be general or targeted towards disclosures of a specific type, for example the US Offshore Voluntary Disclosure Programs.

66. The results of such voluntary disclosure programmes can bring significant amounts of revenue to tax administrations, some figures of which are highlighted in the latest 10th Anniversary Report of the Global Forum on Transparency and Exchange of Information for Tax Purposes (OECD, 2019, p. 32[16]):

> *As of November 2019, voluntary disclosure programmes and tax investigations helped to identify about EUR 102 billion in additional revenue (tax, interest, penalties). Voluntary disclosure programmes have been the largest contributor to this figure with nearly 40 jurisdictions having reported some form of disclosure between 2009 and 2019. For instance, voluntary disclosures brought EUR 462 million in Australia, EUR 13.6 billion in Brazil, nearly EUR 6 billion in Germany, EUR 29 million in Hungary, EUR 54 million in Luxembourg and over EUR 900 million in Mexico. Over 1 million of taxpayers have come forward to voluntarily disclose their assets.*

67. Voluntary disclosure facilities are not just an opportunity to increase compliance amongst taxpayers and improve revenue receipts, but they can also be an opportunity to identify professional enablers. Information collected can be analysed to identify prolific enablers suitable for investigation, as well as increasing understanding of the scale and nature of the threats. Analysis of the structures used in disclosed affairs can be used for risking and for improving regulation and legislation, for example by closing loopholes. There is also the additional deterrent effect if professionals know that their names could be disclosed through such facilities and action potentially taken against them.

4.2.2. Whistleblowers, anonymous sources and other reporting mechanisms

68. Anonymous tip-offs and whistle-blowers have led to successful investigations in many countries, and continue to be a useful source of intelligence in an environment where there is increasing public discontent with tax evaders and those who enable them. In Australia, a publicly accessible tip-off mechanism was created to specifically report on tax evasion schemes and their promoters (ATO, 2019[17]). This voluntary reporting mechanism is openly available online, and creates the opportunity for tax authorities to receive increased intelligence on newly marketed tax schemes or new promoters, as well as a range of other issues. The prospect of being reported upon can result in a decrease in mass-marketed tax schemes, especially by bigger firms concerned with reputational risk.

69. Some countries also provide incentives to those who come forward with information that assists in the successful investigation of a case, such as through a reward or percentage of assets recovered from a successful prosecution, or immunity from prosecution for the whistle-blower. For example, in Mexico, the National Code of Criminal Procedure was amended to allow whistle-blowers to be granted immunity from prosecution, even where the person has participated in a tax or financial crime, if the whistle-blower provides essential information for the prosecution of the ultimate beneficiaries of crimes. To enable these informants to come forward, countries are recommended to have easily accessible mechanisms for sources to make their reports, and appropriate legal and administrative safeguards to protect the anonymity of the individual and the confidentiality of the information provided (OECD, 2017[18]).

4.3. Mandatory disclosure rules

Mandatory disclosure rules are laws put in place by countries that require intermediaries or taxpayers to report to the authorities if they have marketed, implemented or engaged in transactions or arrangements with particular hallmarks. These hallmarks can be designed to capture information such as cross-border aggressive tax planning, offshore structures, and arrangements that circumvent reporting under the AEOI Standard or conceal beneficial ownership.

70. With timely reporting on these arrangements through mandatory disclosure rules, tax authorities are able to intervene earlier on in the life cycle of the commission of tax crimes, before arrangements have been implemented and harmful effects have taken place. Furthermore, the mandatory requirement to report on such arrangements has a disruptive effect on professional enablers who must actively contemplate their actions in the context of the reporting requirements, or who may be deterred from pursuing illegal arrangements due to the reporting requirements. Failure to report can also serve as the basis for specific criminal or civil action. It can also act as a deterrent to clients, if they are informed that the contemplated arrangement will be reported to the tax authority.

71. The 2018 OECD report on Model Mandatory Disclosure Rules for CRS Avoidance Arrangement and Opaque Offshore Structures contain model frameworks and best practices that can assist countries in designing a disclosure regime that fits their needs.[7]

72. For example, since the adoption of *Council Directive (EU) 2018/822* by EU Member States, most EU countries have now either put in place or are in the process of putting in place national legislation for mandatory disclosure rules, which contain significant penalties for failures to comply. Under the Directive, there will also be periodic automatic exchanges of information between EU member states, which can be fed into domestic professional enabler risk assessments and analytics.

73. Where mandatory disclosure is reported to the tax administration, this information should be shared with the relevant tax crime investigators so that they can assess whether there is a scheme that is of a potential criminal nature that ought to be investigated and pursued If this is in a separate agency, a mechanism for sharing this information should be put in place, as part of the whole-of-government approach set out in chapter 5 below.

[7] Although designed in a different context, the 2015 OECD BEPS Action 12 report on Mandatory Disclosure Rules may also provide useful background.

5 Effective investigations: across government and across borders

No single law enforcement agency acting alone can comprehensively tackle the issue of professional enablers, who operate across a range of fields and across borders. To close the gap, silo approaches need to be discarded, and instead tax crime authorities must work collaboratively with other agencies in their own jurisdiction as well as with other agencies internationally. This chapter highlights whole-of-government and multilateral approaches specifically tackling professional enablers.

5.1. Domestic whole-of-government approaches

Different government agencies are involved at various stages of tackling financial crimes, including the prevention, detection, investigation and prosecution of offences and the recovery of the proceeds of crime (OECD, 2017[19]). As such, different agencies will have interactions with, supervision of, or active investigations into professional enablers. This can include tax authorities, financial regulators, financial intelligence units, police and prosecutors.

74. In order to have the most coherent and robust approach to preventing, identifying, disrupting and prosecuting professional enablers, mechanisms should be in place to enable information sharing between the relevant agencies. To start with, this should include mechanisms for reporting and sharing suspicions that an intermediary is a professional enabler. It should also include the broadest possible forms of information sharing, from spontaneous sharing of intelligence, exchanging detailed case information where requested, and, for relevant sets of data, automatic direct access to information (such as a register of disqualified directors, list of known professional enablers or associated actors, or list of known schemes marketed by professional enablers).

75. To implement this most effectively, countries should:

- Put in place legal gateways for reporting and information sharing between agencies;
- Map the existing information held by each agency in connection with professional enablers, in order to determine what types of information will be of relevance to other agencies;
- Train and increase awareness of the role of, and information held by, other agencies as concerns professional enablers, to inform the ability to effectively share information;
- Identify a lead contact in each agency for receiving and disseminating reports of suspicions of professional enabler activity;
- Provide operational guidance for how to request information from, and share information with, other agencies, such as describing the relevant procedures, and developing standard templates in which information should be shared to facilitate easy and efficient information sharing;

- Have a monitoring mechanism for sharing feedback on the results of the shared information, to inform revisions to the operational guidance;
- Have the ability in law and in practice to protect the confidentiality of information and the integrity of work carried out by other agencies.

76. Beyond information sharing, more active, case-specific mechanisms for implementing a whole of government approach to professional enablers are important. These should include:

- ***Joint investigation teams***: these enable agencies with a common interest to work together in an investigation. This enables a multi-disciplinary approach, allowing investigators to draw on a wider range of investigatory expertise, skills and experience. Joint investigations may also help to avoid duplication arising from parallel investigations, and increase efficiency by enabling officials from each agency to focus on different aspects of an investigation. For example, where a professional enabler was devising schemes to commit tax evasion by creating fraudulent refund claims, and then creating false business transaction records to launder the money, a joint tax and money laundering investigation could assist in gathering all relevant evidence efficiently to secure both the tax evasion and money laundering conviction, and raise awareness between the agencies of the mutual links between these crimes.
- ***Inter-agency centres of intelligence***: these centralise information gathering and analysis from a number of agencies. They can gather and analyse existing data held by a range of agencies as well as conduct their own research. Centralising these activities allows for the development of expertise in one area, and can reduce costs of duplication. For example, a centre of intelligence could be tasked with analysing data from offshore leaks to identify high-risk professional enablers operating in the jurisdiction, which could be shared with all relevant agencies to inform future investigations.
- ***Secondments and co-location of personnel***: these arrangements allow the temporary reassignment of officials to other agencies. It is an effective way of transferring skills, building contacts to assist co-operation in the future, and cross-fertilising relevant experience and specialist knowledge. This can be particularly effective in informing officials of the information and powers available to the counterpart agencies, and can make the other forms of information sharing and co-operation more effective.
- ***Whole-of-government training programmes***: Training programmes that bring together officials from a range of agencies provide an important opportunity for building personal relationships and sharing experiences in dealing with common problems. Targeted whole of government training programmes focusing on professional enablers is a way to share information on trends, guidance on investigative techniques, best practice in managing cases and methods for identifying concerns of relevance to another agency.

77. In devising their professional enabler strategy, countries should seek to make the most use possible of a whole-of-government approach to the issue.

Box 21. The United Kingdom's National Economic Crime Centre

Formed in November 2018, the National Economic Crime Centre (NECC) is a collaborative, multi-agency centre that has been established to deliver a step change in the response to tackling economic crime and illicit finance. The NECC brings together law enforcement agencies, prosecutors, government departments and regulatory bodies in the United Kingdom, and sets priorities that informs operational activity.

As an example, in mid-2019, the NECC, in response to the threat from professional enablers, created the Enabler Practitioners Group. This multiagency forum promotes the identification of cases and encourages investigators and prosecutors to use the full range of legislative and regulatory powers. Strategically, the NECC facilitates information sharing with the private sector, which is strengthening the United Kingdom's understanding of the threat and is informing policy on these enablers of financial crime.

5.2. International co-operation

Financial crimes, including tax crimes, are a global problem that needs a global solution. With globalisation, the ability for professional enablers to operate cross-border and arrange transactions that send funds abroad instantly has increased. However, law enforcement authorities have less knowledge of activity outside their borders. International co-operation is therefore an essential aspect of tackling professional enablers. This includes traditional exchange of information channels, as well as newer forms of real-time international co-operation.

5.2.1. Exchange of information

78. Over 160 jurisdictions worldwide have joined the Global Forum on Transparency and Exchange of Information for Tax Purposes (Global Forum) and made a commitment to ensure an effective implementation of the international standards on transparency and exchange of information for tax purposes. The networks for exchanging information have expanded at unprecedented speed, and the ability to request information from almost any country around the world has been made possible through bilateral and multilateral exchange of information and co-operation agreements, such as the Multilateral Convention on Mutual Administrative Assistance in Tax Matters which now covers more than 130 jurisdictions (OECD, 2020[20]).

79. Over the last ten years, the volume of the information exchanged between tax authorities, both on request and automatically, has significantly increased, with more than 250 000 requests being made in this time. In addition, nearly 100 jurisdictions are exchanging information automatically on financial assets held around the world. Nearly 100 countries carried out automatic exchange of information in 2019, enabling their tax authorities to obtain data on 84 million financial accounts held offshore by their residents, covering total assets of EUR 10 trillion. This represents a significant increase over 2018 – the first year of such information exchange – where information on 47 million financial accounts was exchanged, representing EUR 5 trillion. The growth stems from an increase in the number of jurisdictions receiving information as well as a wider scope of information exchanged (OECD, 2020, p. 5[21]).

80. This shows that a commitment to using the exchange of information tools, supported by the accountability mechanism of the Global Forum, opens up an enormous possibility for international co-operation, as well as creating deterrence for professional enablers. In this era of tax transparency, studies

show that there has been a marked effect in the global decline of foreign-owned bank deposits in international financial centres, which fell by 24% (USD 410 billion) between 2008 and 2019 (O'Reilly, Parra Ramirez and Stemmer, 2019[22]).

81. It also means that professional enablers have much more limited scope to operate outside the purview of tax authorities. As part of a professional enabler strategy, countries should be seeking to make the most of this powerful tool, and should continue to provide swift assistance to their counterpart authorities to reduce globally the impact of professional enablers. Countries should also look to broaden their use of exchange of information where possible. For example, most exchange of information agreements allow for:

82. ***Group requests***: countries can request information from a counterpart tax authority about a group of taxpayers even if they are not individually identified. This can be particularly relevant where a professional enabler in the counterpart country has actively contributed to tax evasion on the part of resident taxpayers in a country, but the identity of the individual clients are unknown. See Annex B for a template group request form, created by the OECD Forum on Tax Administration's JITSIC programme. An example from the OECD Model Tax Convention illustrates this (OECD, 2017, p. 493[23]):[8]

> *Financial service provider B is established in State B. The tax authorities of State A have discovered that B is marketing a financial product to State A residents using misleading information suggesting that the product eliminates the State A income tax liability on the income accumulated within the product. The product requires that an account be opened with B through which the investment is made. State A's tax authorities have issued a taxpayer alert, warning all taxpayers about the product and clarifying that it does not achieve the suggested tax effect and that income generated by the product must be reported. Nevertheless, B continues to market the product on its website, and State A has evidence that it also markets the product through a network of advisors. State A has already discovered several resident taxpayers that have invested in the product, all of whom had failed to report the income generated by their investments. State A has exhausted its domestic means of obtaining information on the identity of its residents that have invested in the product. State A requests information from the competent authority of State B on all State A residents that (i) have an account with B and (ii) have invested in the financial product. In the request, State A provides the above information, including details of the financial product and the status of its investigation.*

83. ***Spontaneous exchange of information***, which allows a tax authority to share information that may be of relevance to a counterpart. This can be powerful in speeding up the disruption of professional enablers, in that it alerts a counterpart to risks that they may otherwise be unaware of, or only uncover years later after conducting their own investigations. For example, spontaneous exchange could be relevant when a tax authority has uncovered the identify of a professional enabler that is operating in the counterpart jurisdiction, has become aware of a particular scheme being marketed to or implemented in the counterpart jurisdiction, or has identified a professional enabler's clients that are resident in the counterpart jurisdiction.

84. ***On-sharing of tax information with other law enforcement agencies***: the Multilateral Convention, and certain bilateral tax treaties, generally restrict the use of internationally exchanged information to tax purposes only. However, recognising the links between tax crimes and other financial crimes such as money laundering and corruption, it is possible for the information received by one party to be on-shared with other agencies and used for other purposes, provided that:

- Such information may be used for those other purposes under the laws of the sending country; and
- The competent authority of that sending country authorises such use.

[8] Commentary on Article 26 paragraph 8(h) in OECD (2017), *Model Tax Convention on Income and on Capital: Condensed Version 2017*, OECD Publishing, http://dx.doi.org/10.1787/mtc_cond-2017-en. See also paragraphs 5.2 and paragraphs 8(e) – 8(h) and 8.1

85. This type of on-sharing can be agreed on a bilateral basis, and can be an effective way of ensuring the advances made in ensuring effective international tax information sharing that has taken place in recent years can also be leveraged, where appropriate, by other law enforcement agencies in disrupting and prosecuting professional enablers. In pursuing this extended potential of exchange of information, due regard must be given to the need to ensure recipient agencies can protect the confidentiality of the information received.

5.2.2. OECD Common Reporting Standard (CRS) Disclosure Facility

In 2017, the OECD launched a disclosure facility on the Automatic Exchange Portal to allow open reporting of potential schemes to circumvent the CRS. This facility is part of a wider process that the OECD has put in place to deal with schemes that purport to avoid reporting under the CRS, so that any actual or perceived loopholes can be systematically analysed and addressed. This disclosure facility continues to be a useful information source to track potential enabler activity in the peddling of CRS avoidance schemes. Where the OECD Secretariat is made aware of a potential enabler risk pertinent to a particular country, this information is shared with the relevant governments.

5.2.3. Joint Chiefs of Global Tax Enforcement (J5)

86. The Joint Chiefs of Global Tax Enforcement (the "J5") is an operational alliance between Australia, Canada, the Netherlands, the United Kingdom and the United States, formed to lead the fight against international tax crime and money laundering, including tackling crypto-currency threats, cybercrime, and targeting the professional enablers who make global tax evasion possible. The group brings together leading tax experience and offshore, crypto and cyber expertise from these countries to share intelligence at speed, build capacity and ultimately carry out joint operational activities. An example of this is contained in Box 23, where the Netherlands and the United States of America hosted "challenge" events, bringing together experts, investigators and data scientists to combine their skills and capabilities collaboratively, which culminated in the prosecution of a fraudulent crypto-asset network scheme.

87. The J5 was formed in 2018 in response to a call to action from the OECD for countries to do more to tackle the enablers of tax crime (HMRC & OECD, 2017[24]). Professional services provided by enablers are constantly evolving, utilising modern technology and increasingly complex ways to hide wealth and illicit gains through the exploitation of offshore structures and financial instruments. All five countries face similar threats from organised crime groups and wealthy offshore tax evaders. The J5's pooled resources and collective efforts means that there is increased insight, data and analytical capability available to the authorities of all five countries, enhancing the individual capabilities of each country simultaneously.

88. The J5 has a work stream specifically dedicated to combatting professional enablers. Each country has shared intelligence on targets they have operating in their own country where there is a multi-jurisdictional interest. These investigations involve sophisticated international enablers of tax evasion, such as global financial institutions and their intermediaries who help taxpayers to hide their income and assets. These highly harmful, high-end enablers of tax evasion were previously thought to be beyond the reach of the member countries.

Box 22. Coordinated day of action by the Joint Chiefs of Global Tax Enforcement

The first major operational activity for the Joint Chiefs of Global Tax Enforcement took place in January 2020 in which a globally coordinated day of action into suspected facilitation of offshore tax evasion was undertaken across the United Kingdom, the United States, Canada, Australia and the Netherlands.

The action occurred as part of a series of investigations in multiple countries into an international financial institution located in Central America, whose products and services were believed to be facilitating money laundering and tax evasion for customers across the globe. It was believed that through this institution, a number of clients were potentially using a sophisticated system to conceal and transfer wealth anonymously to evade their tax obligations and launder the proceeds of crime.

The coordinated day of action involved evidence, intelligence and information collection activities such as search warrants, interviews and subpoenas. Significant information was obtained as a result and investigations ensued, with the potential for further criminal, civil and regulatory action to arise from these actions in each country.

Box 23. BitClub network case

Example of crypto-asset fraud facilitated by a professional enabler (IRS, 2020[25]) (DOJ, 2020[26])*

From April 2014 through December 2019, the BitClub Network was a fraudulent scheme that solicited money from investors in exchange for shares of purported crypto-asset mining pools and rewarded investors for recruiting new investors into the scheme. The crypto-asset mining scheme was worth at least USD 722 million in damages to investors.

IRS Criminal Investigation (IRS-CI) special agents worked the case under the umbrella of the Joint Chiefs of Global Tax Enforcement (J5). In November 2019, IRS-CI hosted a crypto "Challenge" in Los Angeles, bringing together investigators, crypto-asset experts and data scientists from the five J5 countries in a co-ordinated push to track down individuals perpetrating tax crimes around the world. During the Challenge, the Dutch Fiscal Intelligence and Investigation Service (FIOD) worked collaboratively with IRS-CI to develop leads in the BitClub Network case.

On July 9, 2020, a Romanian citizen living in Germany has admitted to conspiring to engage in wire fraud and offering and selling unregistered securities in connection with his role in the BitClub Network. He assisted in the creation and operating of the BitClub Network and served as its programmer. In this capacity, he used his professional skills to falsify figures displayed as Bitcoin mining earnings to make it appear that the BitClub Network was earning more than what was actually being mined, effectively acting as a professional enabler for crypto-asset fraud.

The defendant now faces a maximum penalty of five years in prison and a fine of USD 250 000 (twice the pecuniary gain to the defendant or loss to the victims). Several other co-conspirators in the scheme are also being prosecuted.

* Note: This example is provided through publicly available information sources.

5.3. JITSIC Data Leaks Group's work on the Intermediaries Disruption Strategy

89. The Joint International Taskforce on Shared Intelligence and Collaboration (JITSIC) brings together 40 of the world's national tax administrations that have committed to more effective and efficient ways to deal with tax avoidance. Although the scope of this work is quite different to this report, which focusses on tax crimes, the model of international co-operation used by JITSIC, and particularly the work undertaken on the intermediaries disruption strategy, can be instructive for similar initiatives that could be undertaken by agencies responsible for tax crimes and law enforcement.

90. The JITSIC platform enables its member countries to share intelligence, actively collaborate on investigations, and conduct joint compliance activities. Members of JITSIC are able to share information and intelligence in an expedited manner through the JITSIC procedures and existing legal frameworks under the appropriate bilateral or multilateral legal instruments.

91. The JITSIC Data Leaks Group (DLG) arose out of the work of the JITSIC Paradise Papers Initial Assessment Group (PPIAG). The DLG was established in 2018 to continue the compliance risk assessment of the Paradise Papers data, released by the International Consortium of Investigative Journalists (ICIJ), with a focus on delivering practical results and to facilitate or recommend actionable compliance strategies for JITSIC members. The DLG was also mandated to collaboratively analyse anticipated and future data leaks on a needs basis.

92. JITSIC's work in this area has identified intermediaries as a high-risk group that would benefit from targeted multilateral compliance efforts. Intelligence gained from the JITSIC Panama Papers project and the PPIAG is that intermediaries often promote and put a number of taxpayers into the same structures. By targeting intermediaries, members can identify a number of similar arrangements more effectively, whilst minimising proliferation and maximising risk detection, treatment and mitigation strategies. Accordingly, the DLG has commenced work on the JITSIC Intermediaries Disruption Strategy (IDS) to target intermediaries through multilateral compliance action.

References

ATO (2019), *Report schemes and promoters*, https://www.ato.gov.au/General/Tax-planning/Report-schemes-and-promoters/ (accessed on 4 March 2020). [17]

DOJ (2020), *Romanian Programmer Admits That He Helped Create Bitclub Network, A Fraud Scheme Worth At Least $722 Million*, https://www.justice.gov/usao-nj/page/file/1293331/download (accessed on 17 September 2020). [26]

DOJ (2014), *Caribbean-Based Investment Advisor Sentenced for Using Offshore Accounts to Launder and Conceal Funds*, https://www.justice.gov/opa/pr/caribbean-based-investment-advisor-sentenced-using-offshore-accounts-launder-and-conceal (accessed on 8 January 2021). [5]

DOJ (n.d.), *Civil Employment Tax Injunctions*, https://www.justice.gov/tax/civil-employment-tax-injunctions (accessed on 4 March 2020). [13]

DOJ (n.d.), *Program to Shut Down Schemes and Scams*, https://www.justice.gov/tax/program-shut-down-schemes-and-scams (accessed on 4 March 2020). [12]

FATF (2019), *Best Practice on Beneficial Ownership for Legal Persons*, Financial Action Task Force, https://www.fatf-gafi.org/publications/methodsandtrends/documents/best-practices-beneficial-ownership-legal-persons.html. [31]

FATF (2019), *Guidance for a Risk-Based Approach for Legal Professionals*, Financial Action Task Force, https://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Legal-Professionals.pdf. [35]

FATF (2019), *Guidance for a Risk-Based Approach for the Accounting Profession*, Financial Action Task Force, https://www.fatf-gafi.org/media/fatf/documents/reports/RBA-Accounting-Profession.pdf. [36]

FATF (2019), *Guidance for a Risk-Based Approach for Trust & Company Service Providers (TSCPs)*, Financial Action Task Force, https://www.fatf-gafi.org/media/fatf/documents/reports/RBA-Trust-Company-Service-Providers.pdf. [37]

FATF (2019), *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, Financial Action Task Force, http://www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html. [9]

FATF (2018), *Concealment of Beneficial Ownership*, Financial Action Task Force, https://www.fatf-gafi.org/publications/methodsandtrends/documents/concealment-beneficial-ownership.html. [32]

FATF (2018), *Professional Money Laundering*, Financial Action Task Force, https://www.fatf-gafi.org/publications/methodsandtrends/documents/professional-money-laundering.html. [33]

FATF (2014), *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, Financial Action Task Force, http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf. [8]

FATF (2013), *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals*, Financial Action Task Force, https://www.fatf-gafi.org/fr/documents/documents/mltf-vulnerabilities-legal-professionals.html. [34]

FATF (2012-2019), *International Standard on Combating Money Laundering and the Financing of Terrorism & Proliferation*, https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf. [7]

Halter, E. et al. (2011), *The Puppet Masters: How the Corrupt Use Legal Structures to Hide Stolen Assets and What to Do About It*, Stolen Asset Recovery (StAR) initiative. World Bank, http://documents.worldbank.org/curated/en/784961468152973030/The-puppet-masters-how-the-corrupt-use-legal-structures-to-hide-stolen-assets-and-what-to-do-about-it. [4]

HMRC & OECD (2017), *Closing Statement of the Fifth OECD Forum on Tax and Crime*, https://www.oecd.org/tax/crime/closing-statement-oecd-forum-on-tax-and-crime-november-2017.pdf. [24]

ICIJ (2020), *Offshore Leaks Database*, https://offshoreleaks.icij.org/ (accessed on 18 September 2020). [1]

IESBA (n.d.), *International Ethics Standard Board for Accountants*, https://www.ethicsboard.org/ (accessed on 4 March 2020). [14]

IMF (2019), *Chapter 2. Curbing Corruption*, International Monetary Fund, https://www.imf.org/en/Publications/FM/Issues/2019/03/18/fiscal-monitor-april-2019. [3]

IRS (2020), *Examples of Abusive Return Preparer Investigations - Fiscal Year 2017*, https://www.irs.gov/compliance/criminal-investigation/examples-of-abusive-return-preparer-investigations-fiscal-year-2017 (accessed on 14 April 2020). [6]

IRS (2020), *Romanian programmer admits that he helped create Bitclub network, a fraud scheme worth at least $722 million*, https://www.irs.gov/pub/irs-utl/j5-media-release-07-09-2020.pdf (accessed on 17 September 2020). [25]

O'Reilly, P., K. Parra Ramirez and M. Stemmer (2019), "Exchange of information and bank deposits in international financial centres", *OECD Taxation Working Papers*, No. 46, OECD Publishing, Paris, https://dx.doi.org/10.1787/025bfebe-en. [22]

OECD (2020), *Base Erosion and Profit Shifting*, https://www.oecd.org/tax/beps/ (accessed on 18 September 2020). [2]

OECD (2020), *Convention on Mutual Administrative Assistance in Tax Matters*, https://www.oecd.org/tax/exchange-of-tax-information/convention-on-mutual-administrative-assistance-in-tax-matters.htm (accessed on 4 March 2020). [20]

OECD (2020), *OECD Secretary-General Tax Report to G20 Finance Ministers and Central Bank Governors - July 2020*, OECD, http://www.oecd.org/tax/oecd-secretary-general-tax-report-g20-finance-ministers-july-2020.pdf. [21]

OECD (2019), *Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors*, OECD Publishing, https://www.oecd.org/tax/crime/money-laundering-and-terrorist-financing-awareness-handbook-for-tax-examiners-and-tax-auditors.pdf. [10]

OECD (2019), *Tax Morale: What Drives People and Businesses to Pay Tax?*, OECD Publishing, https://www.oecd.org/tax/tax-morale-f3d8ea10-en.htm. [15]

OECD (2019), *Transparency and Exchange of Information for Tax Purposes: Multilateral Co-operation Changing the World*, OECD Publishing, https://www.oecd.org/tax/transparency/global-forum-10-years-report.pdf. [16]

OECD (2018), *Model Mandatory Disclosure Rules for CRS Avoidance Arrangements and Opaque Offshore Structures*, OECD Publishing, https://www.oecd.org/tax/exchange-of-tax-information/model-mandatory-disclosure-rules-for-crs-avoidance-arrangements-and-opaque-offshore-structures.htm. [30]

OECD (2018), *Standard for Automatic Exchange of Financial Account Information in Tax Matters: Implementation Handbook*, OECD Publishing, https://www.oecd.org/ctp/exchange-of-tax-information/implementation-handbook-standard-for-automatic-exchange-of-financial-account-information-in-tax-matters.htm. [27]

OECD (2017), *Effective Inter-Agency Co-Operation in Fighting Tax Crimes and Other Financial Crimes - Third Edition*, OECD Publishing, https://www.oecd.org/tax/crime/effective-inter-agency-co-operation-in-fighting-tax-crimes-and-other-financial-crimes.htm. [19]

OECD (2017), *Model Tax Convention on Income and on Capital: Condensed Version 2017*, OECD Publishing, http://dx.doi.org/10.1787/mtc_cond-2017-en. [23]

OECD (2017), *The Detection of Foreign Bribery, Chapter 2. The Role of Whistleblowers and Whistleblower Protection*, OECD Publishing, http://www.oecd.org/corruption/anti-bribery/OECD-The-Role-of-Whistleblowers-in-the-Detection-of-Foreign-Bribery.pdf. [18]

OECD (2016), *Exchange of Information on Request: Handbook for Peer Reviews 2016-2020 Third Edition*, OECD Publishing, http://www.oecd.org/tax/transparency/global-forum-handbook-2016.pdf. [28]

OECD (n.d.), *Co-operation and exchange of information on ATP*, https://www.oecd.org/ctp/aggressive/co-operation-and-exchange-of-information-on-atp.htm (accessed on 5 June 2020). [11]

OECD/FATF (2011), *Identification and Quantification of the Proceeds of Bribery: A joint OECD-StAR Analysis*, OECD Publishing, https://star.worldbank.org/publication/identification-and-quantification-proceeds-bribery. [41]

OECD/IDB (2019), *A Beneficial Ownership Implementation Toolkit*, OECD Publishing, http://www.oecd.org/tax/transparency/beneficial-ownership-toolkit.pdf. [29]

StAR (2012), *On the Take: Criminalizing Illicit Enrichment to Fight Corruption*, World Bank Publications, https://star.worldbank.org/publication/take-criminalizing-illicit-enrichment-fight-corruption. [38]

StAR (2012), *Politically Exposed Persons: Preventive Measures for the Banking Sector*, World Bank Publications, https://star.worldbank.org/publication/politically-exposed-persons. [40]

StAR (2012), *Public Office, Private Interests: Accountability through Income and Asset Disclosure*, World Bank Publications, https://star.worldbank.org/publication/public-office-private-interests. [39]

StAR (2011), *Asset Recovery Handbook: A Guide for Practitioners*, World Bank Publications, https://star.worldbank.org/publication/asset-recovery-handbook. [45]

StAR (2011), *Barriers to Asset Recovery: An Analysis of the Key Barriers and Recommendations for Action*, World Bank Publications, https://star.worldbank.org/publication/barriers-asset-recovery. [44]

StAR (2010), *Stolen Assets Recovery: Towards a Global Architecture for Asset Recovery*, Stolen Assets Recovery Initiative, https://star.worldbank.org/publication/towards-global-architecture-asset-recovery. [42]

StAR (2009), *Stolen Asset Recovery: A Good Practice Guide for Non-conviction-based Asset Forfeiture*, World Bank Publications, https://star.worldbank.org/publication/towards-global-architecture-asset-recovery. [43]

StAR (2009), *Stolen Asset Recovery: Management of Returned Assets*, StAR, https://star.worldbank.org/publication/management-returned-assets. [46]

The Egmont Group (2013), *The Role of Financial Intelligence Units in Fighting Corruption and Asset Recovery: An Egmont Group White Paper*, The Egmont Group, https://egmontgroup.org/en/filedepot_download/1661/55. [47]

The Egmont Group (2011), *Enterprise-wide STR Sharing: Issues and Approaches*, The Egmont Group, https://egmontgroup.org/en/filedepot_download/1661/47. [48]

UNODC (2017), *Effective management and disposal of seized and confiscated assets*, United Nations Office on Drugs and Crime, https://www.unodc.org/documents/corruption/Publications/2017/17-07000_ebook_sr.pdf. [49]

UNODC (2012), *Manual on International Cooperation for the Purposes of Confiscation of Proceeds of Crime*, United Nations Office on Drugs and Crime, https://www.unodc.org/documents/organized-crime/Publications/Confiscation_Manual_Ebook_E.pdf. [50]

UNODC (2011), *Handbook on Identity-related crime*, United Nations Office on Drugs and Crime, https://www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf. [51]

Annex A. Other related work

This report is intended to be a contribution to the work of the international community to building strong, inclusive and fair societies, by strengthening the ability of policy makers and law enforcement authorities to address risks that undermine society. Significant work has been undertaken by other bodies, which will also be of relevance in this area. This includes:

In the tax area:

- the work of the Global Forum on Transparency and Exchange of Information, including to drive the effectiveness of exchange of information tools between tax authorities, as well as improving transparency (OECD, 2018[27]) (OECD, 2016[28]) particularly in the area of beneficial ownership (OECD/IDB, 2019[29]);
- the work of the Committee on Fiscal Affairs, including to provide guidance on the available legal mechanisms for exchange of information and multilateral co-operation in tax matters, such as its recent work on model mandatory disclosure rules (OECD, 2018[30]);
- the work of the Forum on Tax Administration, including its Joint International Taskforce on Shared Intelligence and Collaboration(JITSIC) which provides a mechanism for tax administrations to exchange information, actively collaborate on investigations, and share strategies and intelligence on operational risks and issues, including its working group on the Data Leaks.

In anti-money laundering, the work of the Financial Action Task Force, including:

- guidance and best practices on beneficial ownership (FATF, 2019[31]);
- concealment of beneficial ownership (FATF, 2018[32]);
- techniques and tools used by professional money launderers (FATF, 2018[33]);
- guidance for legal professionals on vulnerabilities for involvement in money laundering and terrorist financing (FATF, 2013[34]);
- guidance for a risk-based approach for legal professionals (FATF, 2019[35]), accountants (FATF, 2019[36]) and trust and company service providers (FATF, 2019[37]).

In anti-corruption, the work of the World Bank's (WB) and the United Nations Office on Drugs and Crime's (UNODC) joint Stolen Asset Recovery Initiative (StAR), including:

- guidance and best practices on the criminalisation of illicit enrichment of public officials (StAR, 2012[38]);
- examining the core design features and implementation challenges of income and asset disclosure (IAD) regimes (StAR, 2012[39]);
- examining the forms of beneficial ownership structures involving high-level public officials and providing recommendations on formulating an anti-corruption strategy (Halter et al., 2011[4]);
- formulating policy recommendations for banks and regulatory authorities to improve preventive measures that address money laundering risks posed by Politically Exposed Persons (PEPs) involved in corruption (StAR, 2012[40]);
- OECD / StAR study on the identification and quantification of the proceeds of active bribery in international business transactions (OECD/FATF, 2011[41]).

In enforcement, the work of

- StAR on asset recovery, including a series of publications on; the role of the international community and national authorities (StAR, 2010[42]), guidance for non-conviction based asset forfeiture (StAR, 2009[43]), the key barriers to asset recovery in foreign jurisdictions and good practices to counter them (StAR, 2011[44]), approaches to recovering proceeds of corruption located in foreign jurisdictions and their underlying challenges (StAR, 2011[45]), and the management of successfully recovered stolen assets (StAR, 2009[46]).
- Egmont Group of Financial Intelligence Units (Egmont) on; the role of financial intelligence units (FIU) fighting corruption and asset recovery (The Egmont Group, 2013[47]), and guidance for cross-border suspicious transaction report (STR) sharing regime (The Egmont Group, 2011[48]).
- UNODC on enforcement issues including; management and disposal of seized and confiscated assets (UNODC, 2017[49]), guidance on international co-operation in asset recovery (UNODC, 2012[50]), and criminalisation and enforcement of identity-related crime (UNODC, 2011[51]).

Annex B. Example of template for Group EOI request

Request for Information under the TIEA/DTC/MAC[9] applicable between [jurisdiction] and [jurisdiction]

The completed form constitutes a confidential communication between the competent authorities governed by [legal basis if applicable].

1.	To: [1]		
2.	From:[2]		
3.	Contact point[3]	Name:	
		Email:	
		Telephone:	
		Language skills:	
4.	Legal Basis:		
5.	Reference numbers and related matters	Reference number: [4]	
		Initial request:	Please tick: ☐ yes ☐ no If no, please provide reference number(s) and date(s) of any related request(s) and/or response(s):
		Number of attachments to the request:	
		Total number of pages for all attachments:	
6.	Urgency of reply	Date, if any, after which information would no longer be useful:	

[9] Please verify that the title corresponds to your agreement and please contact the requested jurisdiction prior to the sending of a group or bulk request.

		Urgent reply required due to:	Please check the box: ☐ Statute of limitation; date: ☐ Suspected criminal tax matter ☐ Court case ☐ Other reasons (please specify):
7.	Summary[5]		
8.	Identity of subject/group under examination or investigation:[6]		
9.	Tax period/s under investigation or taxable event for which or in relation to which the information is sought:[7]		
10.	Tax(es) to which the request relates:[8]		
11.	Purpose in accordance with the applicable EOI instrument, for which the information is requested:		Please check one or more boxes: ☐ determination, assessment and collection of taxes of civil/administrative tax matters[9], ☐ investigation or prosecution of criminal tax matters, ☐ other (please specify):
12.	Relevant background:[10]		
13.	Explanation to confirm that all possible domestic means have been pursued to obtain the information requested, except those that would give rise to disproportionate difficulties:[11]		
14.	Reasons why the information requested is foreseeably relevant for the tax purpose indicated/investigation:[12]		
15.	Information requested:[13]		

16.	Grounds for believing that the requested information is held in the requested jurisdiction or is within the possession or control of a person within its jurisdiction:	
17.	Name and address of any person believed to be in possession of the information requested (to the extent known):	
18.	Request to refrain from notifying the persons under investigation or concerned:	Please tick: ☐ yes ☐ no Please indicate reasons: ☐ If yes, the authority responsible in the requesting state confirms that it would be able to guarantee this course of action in similar circumstances.
19.	Form, if any, in which information is requested:[14]	In the case of the production of copies, authentication is required: Please tick: ☐ yes ☐ no If yes, which ones: Further requirements, such as translation of reply: Please tick: ☐ yes ☐ no If yes, which ones:
20.	In making the request, the requesting competent authority states that: (a) all information received in relation to this request will be kept confidential and used only for the purposes permitted in the agreement which forms the basis for this request; (b) the request is in conformity with its law and administrative practice and is further in conformity with the agreement on the basis of which it is made; (c) the information would be obtainable under its laws and in the normal course of its administrative practice in similar circumstances.	

Date

Authorised signature of requesting competent authority

Foonotes for sending country guidance only. Please remove before sending.

[1] Please add name and address of the competent authority of the requested jurisdiction.

[2] Please add name and address of the competent authority of the requesting jurisdiction.

[3] The contact point having the authority to exchange information.

[4] Please provide a reference number that the requested competent authority could use in case of questions and that allows retrieving the request and the related file.

[5] Please give a short and concise request description regarding the tax purpose of the investigation and the purpose of request.

[6] Please refer to the commentary to Article 26 of the OECD Model Convention (DTC), especially to the paragraphs related to group request, e.g. paragraphs 5.2 and paragraphs 8(e) – 8(h) and 8.1.

[7] Please verify that the applicable EOI instrument is in place and in force for the period of the request and the period under review. For older years, if prosecution or assessment would ordinarily be proscribed by the applicable statute of limitations, please describe how the limitations period is held open, or is expected to be held open.

[8] Please review the applicable EOI instrument and add the name of the tax(es), e.g. corporate income tax. Add also the type of tax(es) (personal, corporate etc.) if the name of the tax(es) is not sufficiently indicative of the type of tax.

[9] It is understood that the investigation of civil/administrative tax matters falls under this heading.

[10] Please provide the necessary background information, which would typically include a brief summary of the ongoing examination or investigation and how the requested information relates to this examination or investigation. The background information should if applicable mention the link regarding a project or other source of information assessed as useful for the administration of the request by the requested jurisdiction. Insert any other factual basis for request, such as information from similar taxpayers' examinations, interviews, or other research, if applicable, as well as the model of behaviour regarding the group.
Where any other persons (e.g. individuals, companies, partnerships, trusts, etc.), including foreign persons, are relevant to the examination or investigation and the request, please specify, to the extent known, their relationship to the taxpayer and provide information sufficient to identify these persons.
Please insert an enclosure showing the scheme/structure, if applicable.
If preferred, please refer to an attachment to provide the Relevant Background alternatively include a summary of the Relevant Background with the full description in an attachment enclosed.

[11] Please provide the necessary information to confirm that all means available within your territory have been pursued to obtain the information, except those that would give rise to disproportionate difficulty. In case you have abstained from using any means available in your own territory to obtain the information because this would give rise to disproportionate difficulties, please provide a description of the means and of the disproportionate difficulties.

[12] Please insert reasons for believing that the information requested is relevant to your investigation. Please refer to the definition of foreseeable relevance in the commentary to Article 26 of the OECD Model DTC, especially to the paragraphs related to group request, i.e. paragraphs 5, 5.1 and 5.2 and 8h, as well as Articles 1 and 5(5) OECD Model TIEA and accompanying commentary. The requirements to meet the standard of "foreseeable relevance" implies the detailed description of the group subject to the request, the facts and circumstances that have led to the request as well as a clear factual basis supporting the reasons to believe that the taxpayers of the group have been non-compliant. Typically, such factual basis could emanate in previous investigations or voluntary disclosure programs. This could include an explanation of the applicable tax law or criminal law, and why there is reason to believe that the taxpayers described have been non-compliant and how the information would assist in determining compliance of the taxpayers described.

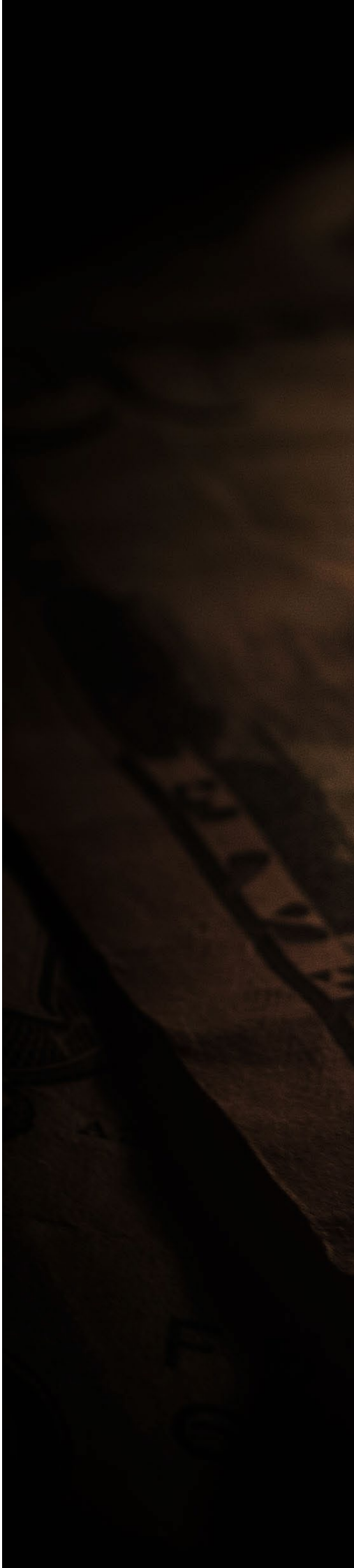
[13] The requested information should be foreseeable relevant and in concordance with the information provided in the previous sections, e.g. Relevant Background. Please be as specific as possible about the information you are requesting, as it will form the basis for any domestic information gathering measures

taken by the requested jurisdiction. For group requests, please consider whether only data/information (no documents) could be sufficient. Please give numbers/letters to the questions to ease their administration.

[14] Please specify the format in which the information is requested and whether any translation of reply, including to which language, or any authentication procedure is needed, as well as the reasons therefore. Please consider the additional time and costs, which might need to be agreed upon, relating to authentication of documents and translation.

Ending the Shell Game:
Cracking down on the Professionals who enable Tax and White Collar Crimes

White collar crimes like tax evasion, bribery, and corruption are often concealed through complex legal structures and financial transactions facilitated by lawyers, accountants, financial institutions and other "professional enablers" of such crimes. These crimes have significant impacts on government revenue, public confidence and economic growth, including the recovery from COVID-19. This report sets out a range of strategies and actions for countries to take to tackle professional intermediaries who enable tax evasion and other financial crimes on behalf of their criminal clients. The report highlights the damaging role played by these intermediaries and the importance of concerted domestic and international action in clamping down on the enablers of crime, and includes recommended counter-strategies for deterring, disrupting, investigating and prosecuting the professionals who enable tax and white collar crimes.



OECD
BETTER POLICIES FOR BETTER LIVES

For more information:

ctp.contact@oecd.org

www.oecd.org/tax/crime

@OECDtax