Policy for Anti-Money Laundering (AML) and Counter Terrorist Financing (CTF)

Policy Purpose

This Policy forms an outline of the work done by Summa Accountancy Services Limited to both identify and prevent the risk of ML/TF (Money Laundering and Terrorist Financing) to the firm. The different steps identified within this policy act in combination with each other and form an integral part of all aspects of Summa Accountancy Services Limited's work.

Consequently, individual sections of the policy should not be read or considered in isolation.

Similarly, Summa Accountancy Services Limited is conscious that for it to have an effective and compliant AML/CTF (Anti-Money Laundering/Counter Terrorist Financing) approach it must follow its own policies and procedures diligently and be clear to document any occasion of variation from its policies and procedures and reasons for such variations. Such controls over the implementation of its policy are crucial.

Following on from this, Summa Accountancy Services Limited has a strict policy of not varying from its own policies and procedures without the documented approval of senior management.

Through documentation of robust compliance with a comprehensive and effective set of policies and procedures Summa Accountancy Services Limited will make every effort possible to be compliant with law and guidance in the areas of ML/TF and to play its part in both the prevention and identification of both money laundering and terrorist financing.

Summa Accountancy Services Limited recognises that the aims of the funding of terrorism is different to those seeking to launder money but is aware that there are many similarities between how the two distinct goals are sought to be achieved. It is, however, clear that this policy, when applied to both its own Firm Risk Assessment and policies and controls, will be the same policies, procedures and controls to achieve the ability to identify and report relevant activity under TACT (Terrorism Act 2000) and POCA (Proceeds of Crime Act 2002).

Regulated Firm Under MLR 2017

Summa Accountancy Services Limited provides services that fall within one or more of the definitions of categories of services which are regulated services within the definitions under Regulation 11 and 12 of The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017) (“the regulations”) as enacted on the 26/06/2017 and as subsequently amended. The Money Laundering and Terrorist Financing (Amendment) Regulations 2019 enacted on 10 January 2020 and The Money Laundering and Transfer of Funds (Information) (Amendment) (EU Exit) Regulations 2019 enacted on the day that the UK left the EU.Further legislative changes include the Sanctions and Anti-Money Laundering Act 2018(Sanctions Act),The Sanctions(EU Exit)(Miscellaneous Amendments)Regulations 2020 and The Money Laundering and Terrorist Financing(Amendment)(EU Exit)Regulations 2020.

2017 regs: http://www.legislation.gov.uk/uksi/2017/692/made

2019 regs update effective 2020: http://www.legislation.gov.uk/uksi/2019/1511/contents/made

2019 EU exit: http://www.legislation.gov.uk/uksi/2019/253/contents/made

2020 EU exit: https://www.legislation.gov.uk/uksi/2020/991/contents/made

2018 Sanctions act: https://www.legislation.gov.uk/ukpga/2018/13/contents

2020 Sanctions amendments: https://www.legislation.gov.uk/uksi/2020/591/contents/made

Definitions of relevant regulated services include:

Auditor

Insolvency Practitioner

External Accountant

Tax Adviser (as amended by the 2020 regs. update)

Trust or Company Service Provider

Schedule of Firm Services

- Bookkeeping
- Payroll
- Auto-Enrolment Administration
- Indirect Tax (Including VAT returns)
- Indirect Tax Advisory (including VAT registration)
- Research and Development Tax Relief
- Tax advisory (direct taxes)
- Tax advice on taxes payable to Non-UK tax authorities
- Tax planning (tax payable to UK tax authorities)
- Tax planning (tax payable to Non-UK tax authorities)
- Accounts preparation - management/cashflow/budgeting
- Accounts preparation - financial statements (Annual Accounts and Reports)
- Filing submission to HMRC / Companies House
- Accounts submission to the proper authority (Charity Commission, ATOL, or overseas tax authorities for example)
- Statutory Audit
- Client Money Auditing
- Charity Independent Examinations
- Business Advice (General)
- Investigations

Summa Accountancy Services Limited Approach to AML/CTF

Summa Accountancy Services Limited is aware that it is obliged to comply with the legislation, guidance and best practice that is in force from time to time in relation to AML/CTF that is relevant to services offered by Summa Accountancy Services Limited.

Summa Accountancy Services Limited is aware of the damage done to people and property through Money Laundering (ML) and Terrorist Financing (TF) and recognises that it has a part to play in both preventing and identifying ML and TF. Laundered money has been described as the oxygen to crime, terrorism and tax avoidance. To cut off the support of oxygen is seen as a key goal of all of those within the regulated sector.

However, Summa Accountancy Services Limited is aware that it is not empowered as a law enforcement agency and must be careful not to overstep its role as set out in the legislation and guidance.

Summa Accountancy Services Limited is committed to a high level of compliance through a robust and wide-ranging approach to AML/CTF compliance that touches on all aspects of Summa Accountancy Services Limited's service provision.

Summa Accountancy Services Limited understands that the principal money laundering offences are laid out in POCA (Proceeds of Crime Act 2002). POCA explains what constitutes both criminal conduct and criminal property. In simple terms, criminal property is the proceeds of criminal conduct (committing a crime).

Summa Accountancy Services Limited is clear that it is what becomes of the criminal property that POCA details as the main money laundering offences. The Firm is also clear that POCA does not just apply to the author of the crime that created the proceeds but to any other persons involved in dealing with those proceeds. It is what happens to the proceeds of crime that is money laundering.

Summa Accountancy Services Limited understands that the Proceeds of Crime Act (2002) (POCA) is very broad in its definitions of money laundering. Part 7 of POCA S.327 (concealing), S.328 (arrangements) and S.329 (acquisition, use and possession) explains the offences that constitutes money laundering in relation to Criminal Property. Here is a link to POCA: https://www.legislation.gov.uk/ukpga/2002/29/contents

Criminal Property is defined in POCA as well as Criminal Conduct.

Criminal Property, in summary, is a person's benefit from Criminal Conduct which in summary is conduct that constitutes an offence in the UK.

Criminal Property, in summary, is a person's benefit from Criminal Conduct which, in summary, is conduct that constitutes an offence in the UK.

POCA 2002 s.340 contains the following:

2) Criminal conduct is conduct which–

a) constitutes an offence in any part of the United Kingdom, or

b) would constitute an offence in any part of the United Kingdom if it occurred there.

3) Property is criminal property if–

a) it constitutes a person's benefit from criminal conduct or it represents such a benefit (in whole or part and whether directly or indirectly), and

b) the alleged offender knows or suspects that it constitutes or represents such a benefit.

From these open definitions it can be seen that there is an all crimes approach to what constitutes relevant criminal conduct in relation to money laundering in UK law, also included are offences that took place

elsewhere and had they taken place in the UK would have been an offence.

For ease of reference the main money laundering offences under POCA 2002 are listed below:

s 327: An offence is committed if a person conceals, disguises, converts, transfers or removes from the jurisdiction property which is, or represents, the benefit of criminal conduct (i.e. the proceeds of crime) and the person knows or suspects represents such a benefit

s 328: An offence is committed when a person enters into or becomes concerned in an arrangement which he knows or suspects will facilitate another person to acquire, retain, use or control benefit from criminal conduct and the person knows or suspects that the property is benefit from criminal conduct

s 329: An offence is committed when a person acquires, uses or has possession of property which he knows or suspects represents benefit from criminal conduct

It should be noted that S.340 (11) of POCA includes planning or attempting an offence under S.327, 328 and 329.

It should be noted that S.340 (11) of POCA includes planning or attempting an offence under S.327, 328 and 329.

(11) Money laundering is an act which—

(a) constitutes an offence under section 327, 328 or 329,

(b) constitutes an attempt, conspiracy or incitement to commit an offence specified in paragraph (a),

(c) constitutes aiding, abetting, counselling or procuring the commission of an offence specified in paragraph (a), or

(d) would constitute an offence specified in paragraph (a), (b) or (c) if done in the United Kingdom.

Summa Accountancy Services Limited is alive to the risk of being involved with the proceeds of crime and, for example, moving or holding third party property which is the proceeds of crime could make it guilty of money laundering. The firm understands that its robust approach to AML/CTF is part of its own defences against being drawn into laundering the proceeds of another person's crime and therefore potentially being guilty of an offence under POCA itself.

Summa Accountancy Services Limited is also aware that it is POCA and TACT that place an obligation on it to identify and make Suspicious Activity Reports (SARs) to the National Crime Agency (NCA).

Summa Accountancy Services Limited is aware that there is no de minimus level for its reporting obligations under POCA and TA. The firm's commitment to its reporting obligations is detailed later in this policy document.

Summa Accountancy Services Limited is not an expert in criminal law relevant in the UK or globally and, as such, realises the flexibility that is introduced by POCA which includes "suspicion" and "grounds for suspicion" as reportable matters alongside "knowledge" or "grounds for knowledge".

Summa Accountancy Services Limited, therefore, recognises matters to be reported include matters where there is a suspicion that conduct has taken place that is known to be a crime and something that has taken place that there is a suspicion is criminal conduct.

What is Risk?

The first UK National Risk Assessment of Money Laundering and Terrorist Financing (NRA) was issued in October 2015. The NRA 2015 provided a useful insight into how the UK HM Treasury and the UK Home Office viewed the state of money laundering and terrorist financing in the UK at the time. A 2nd NRA was issued in October 2017 which builds on 2017. The 2017 NRA recognises the same factors that make the UK attractive for legitimate financial activity make it attractive for criminals and terrorists.

The latest NRA was published on 17 December 2020. The NRA 2020 is an excellent document, and it is strongly recommended as an important document to read. Your firm needs to be aware of the NRA - part of your own business' risk assessment should take account of its contents, taking account of its finding is imperative for your business' ongoing success.

https://www.gov.uk/government/publications/national-risk-assessment-of-money-laundering-and-terrorist-financing-2020

Summa Accountancy Services Limited awaits the release of the next National Risk Assessment and will review its approach to and implementation of measures to identify and prevent money laundering and terrorist financing in the light of the information contained within the next National Risk Assessment.

Listed below is an extract from the NRA 2020 which includes a breakdown of how risk is recognised along with some key definitions used within the document; these definitions are very useful in highlighting the interaction of key terms used within the firm's approach to risk.

Annex A

Methodology

1.6 The methodology used for the 2017 NRA was similar to that used for the 2017 NRA. This follows the 3 key stages identified in FATF guidance, of identification, assessment and evaluation of evidence within the context of the ‘Management of Risk in Law Enforcement (MoRiLE) model. The same methodology has been used for both the money laundering and terrorist financing elements of this assessment.

1.7 Several key terms used throughout the assessment are defined below:

- Threat - This covers the intent and capability of people to cause harm, and the activities they conduct to do so: money laundering threats include predicate offences and criminals who commit them, while terrorist financing threats include those groups and individuals conducting terrorist activity.
- Vulnerability - These are inherent things that can be exploited by threat actors: see below for the full list of vulnerabilities we refer to throughout the NRA.
- Consequence - The impact or harm that money laundering or terrorist financing may cause, including the effect of the underlying criminal and terrorist activity on financial systems and institutions.
- Likelihood - How much money laundering or terrorist financing we assess is actually happening in a sector.
- Mitigations - These are the actions that are taken to reduce the risk. This includes the effectiveness, capability and capacity of firms within each sector, supervisors and law enforcement.

1.8 The first stage of the assessment focused on identifying evidence which had emerged since the last NRA was conducted in 2017. This included evidence submitted by law enforcement agencies, government departments, supervisors, firms and non-governmental organisations, as well as other published evidence. After

collecting and reviewing this evidence, further evidence was gathered to fill gaps identified. Calls for evidence were issued to all supervisory bodies and to firms in all sectors, and roundtables or bilateral meetings were held to follow these up where possible. Altogether, this resulted in contributions submitted by over 100 organisations across the different sectors considered.

1.9 The next stage involved analysing the data provided by stakeholders to establish the risks present, assess the likelihood of them materialising, understand their impact, and assess the effectiveness of mitigations. We used the evidence for all sectors, activities or products to make an evaluation of the following risk factors under the categories of vulnerability, likelihood and mitigation. We used an adapted MoRiLE model to establish money laundering and terrorist financing risk rankings for each area. The MoRiLE model evaluates inherent risk, based on vulnerabilities and the likelihood of criminals or terrorists exploiting these, followed by evaluating mitigating factors to calculate the net risk in an area. 1.10 Given the largely hidden nature of money laundering and terrorist financing, the evidence used to assess these risk factors relies on a combination of hard data, case studies and expert judgment from law enforcement agencies, supervisory authorities and those responsible for AML/CTF within firms.

Table 1.A: MoRiLE model used to establish risk ratings

MoRiLE Category	Risk Factor
Vulnerabilities	Levels of transparency and anonymity in the sector
	The complexity of the product or service
	The level of exposure of the product or service to high-risk persons or jurisdictions
	Speed with which transactions relating to the product or service can be completed
	Typical volume and frequency of transactions relating to the product or service
	Accessibility of the product or service
Likelihood	An assessment of scale of money laundering or terrorist financing, including consideration of the intent and capability of actors
	Capacity and capability of law enforcement agencies to mitigate the money laundering or terrorist financing risks around the product or service
Mitigations	Capacity and capability of supervisors or regulators to mitigate the money laundering or terrorist financing risks around the product or service
	Capacity and capability of firms to mitigate the money laundering or terrorist financing risks around the product or service

1.11 Throughout the NRA, we will refer to these vulnerabilities and the likelihood and mitigations when discussing the risks.

1.12 Our assessments have been extensively reviewed by money laundering and terrorist financing experts across government, law enforcement, supervisors and the private sector. Therefore, the findings of this NRA reflect our collective understanding of the risks.

1.13 It should be noted that the risk rating is a relative assessment, and a rating of low risk does not mean that there is no risk within a sector. Money laundering and terrorist financing may still take place through low risk sectors at a significant level and all sectors or areas covered are assessed to be exposed to some level of risk. It is also important that the narrative is read alongside the headline risk ratings, to fully understand the risks posed.

1.14 All chapters should be read. The multifaceted nature of money laundering and terrorist financing means that several sectors could be involved in one money laundering case. It is important to understand the interconnected nature of various sectors, and how controls at each and every stage in the process strengthens our

defences against abuse. Throughout the NRA, we signpost connections to other sectors that you should refer to.

Accountancy Service Providers (ASPs) is the title given to those who are regulated for AML/CTF in the sector within which Summa Accountancy Services Limited operates.

The NRA 2015 lists the ASP sector as the sector with the second highest risk in the UK of money laundering and in particular had the highest risk of all sectors for the likelihood of money laundering taking place.

The NRA 2020 rates the risk of exposure to ML in the accountancy sector as high, which is the same as the rating in the 2017 NRA.

The NRA 2020 rates the risk of exposure to TF in the accountancy sector as low, which is the same as the rating in the 2017 NRA.

Summa Accountancy Services Limited is aware that the risk assessment of the sector within which it works is not static and it is recognised that steps to stay up to date with the changing risk profile and relevant risk to this sector.

NRA 2020 explains details of the risks relevant to the accountancy sector and an extract is included below:

Chapter 9

Accountancy services

Summary and risks

- Accountancy Service Providers (ASPs) monitored under the Money Laundering Regulations (MLRs) offer a wide range of services and are either supervised by the Professional Body Supervisors (PBSs) or by HM Revenue & Customs (HMRC).1
- Overall, the risk of money laundering through ASPs remains high. The risk is highest when ASPs do not fully understand the money laundering risks and do not implement appropriate risk-based controls, particularly where ASPs fail to register with a supervisor.
- Accountancy services remain attractive to criminals due to the ability to use them to help their funds gain legitimacy and respectability, as implied by ASPs' professionally qualified status. Those providing accountancy services remain at risk of being exploited or abused by criminals, especially if ASPs become complacent in their regulatory obligations under the MLRs, or willingly facilitate money laundering. The accountancy services considered most at risk of exploitation continue to be company formation and termination, mainstream accounting and payroll. While there have been improvements in the supervision of ASPs, in part due to the work of the Office for Professional Body Anti-Money Laundering Supervision (OPBAS), these services remain prevalent in law enforcement cases.
- We continue to judge that accountancy services are not attractive for terrorist financing, and there remains no evidence of these services being abused by terrorists. Therefore, the risk of terrorist financing through the sector is assessed to be low.

If a practitioner is undertaking regulated activity under the MLRs, they should be registered with PBSs or HMRC. However, as the term accountant is not protected and those practicing in the profession do not have to be registered with a supervisor for the majority of their accountancy activity, there is a risk that unsupervised practitioners carry out AML regulated business.

Trust and company service providers (TCSPs)Company formation and associated TCSP services[2] continue to be the highest risk services provided by ASPs for money laundering. These can enable the laundering of millions of pounds, conceal the ownership of criminal assets and facilitate the movement of money to secrecy jurisdictions. Of the 23,400 TCSP providers in the UK, 72% are supervised by accountancy bodies; however most provide these services as an add on to their main accountancy services.

9.2 Company formation as a standalone service offers less exposure to potential abuse and it is therefore considered lower risk. However, when coupled with other high-risk services or high-risk factors, such as a third party outside of the UK, the level of risk increases. For example, a UK service provider was asked by a corporate service provider in another jurisdiction to set up a UK company. The risk was assessed based on the corporate service provider, rather than the underlying client. This resulted in the risk assessment on their part being lower than it should be and the TCSP not asking for business reasons as to why the client wanted to set up a company in the UK for revenues of £12,000.

9.3 ASPs that offer registered office or nominee directorship services are also at risk of exploitation for money laundering as those services can enable concealment of beneficial ownership or be used to facilitate the movement of money to offshore jurisdictions. Companies House acknowledge the issues surrounding beneficial ownership transparency in the UK and are taking steps to prevent the system being abused. See paragraphs 9.25 and

11.30 below for more information on the steps being taken by Companies House to mitigate this risk. See chapter 11 on trusts and corporate structures for more detail on the risks associated with company formation and other trust and company services ASPs may offer.

2 The MLRs define a TSCP as a firm or sole practitioner which by way of business, forms companies or other legal persons; acts as or arranges for someone else to act as a company director, partner or nominee shareholder; provides a registered office or business address or similar; and/or acts as or arranges for someone else to act as a trustee for a trust or similar arrangement. The provision of TCSP services involves various professional service sectors including ASPs, many of which provide these services as add on services to their core business activity.

Mainstream accounting

9.4 False accounting continues to pose a high risk of money laundering, as it can enable criminals to mask the source of funds, often in large amounts. This can fall into 3 categories: false bookkeeping, production of false documents and audit. We consider audit to pose a lower risk of money laundering abuse due to the strict parameters placed on ASPs undertaking these services.

9.5 Bookkeepers can enable money laundering by transferring money or creating paperwork to legitimise the flow of funds, both unwittingly and knowingly. This can include trade-based money laundering, where invoices are created in the absence of a sale, or invoices inflate the value of goods sold. Records can also be created to hide the existence of taxable assets. This can legitimise large amounts of illicit funds. See paragraph 9.10 for more on placement of tax evasion proceeds. However, ASPs don't always have to be complicit in this activity to enable money laundering. Legitimate ASPs may fail to identify

receipts that their client has falsified or present an inaccurate picture. An ASP with poor MLR compliance can heighten their exposure to this risk, as it reduces the opportunities to identify red flags.

9.6 ASPs are often relied upon to produce or verify documents relating to financial positions, for use in applications such as mortgages, loans or visas. There is a risk that these services will be exploited by criminals to facilitate money laundering. ASPs could be used for their status as a trusted professional to produce falsified financial positions or legitimise criminal assets. Mitigations may include robust client due diligence procedures,

but there are concerns that transactions are often overly complicated, and ASPs are not always scrutinising the authenticity of provided documentation and the underlying financial data.

9.7 Audit services can provide an additional layer of legitimacy to accounts and documents, and there is evidence that this has been used by criminals to launder millions of pounds.3 However, it is highly unlikely to be used frequently for laundering due to the high barrier to entry to both access and provide audit services. Unlike other services offered by ASPs, authorisation from a supervisory body is required to perform audit services and strict monitoring conditions and protocols are imposed. Likewise, The Companies Act 2006 only requires the audit of certain companies with turnover and/or assets of several million pounds; companies of this size are more likely to have robust internal accounting procedures, making it harder to hide large scale laundering.

Payroll services

9.8 As with false accounting, payroll services can also provide criminals with a legitimate-looking record of money movement. We assess the risk of payroll services being used to launder funds is high due to poor mitigations in place. This may include poorly anti-money laundering (AML) trained staff providing these services, services provided by non-customer facing staff, and a lack of information provided to payroll providers by the customer to identify suspicious activity.

Other risks

9.9 The provision of tax advice and acting as an agent with HMRC on behalf of clients provides several means to launder money and poses a high risk. This is because large amounts of funds can be claimed or undeclared and there is a high likelihood of this service being used.

9.10 ASPs can advise clients on how to under-represent their turnover or income to reduce their tax liabilities. While this behaviour is primarily fraud (making a gain through false representation), it also counts as enabling money laundering. This is because the gain obtained (money retained that would otherwise be paid toward a tax liability) is then the proceeds of crime that is placed in the financial system. Likewise, ASPs can reclaim money from HMRC on a client's behalf when not entitled to do so. This places the proceeds of crime in the financial system as the fraudulently gained funds will be transferred to the client's control as an apparently legitimate refund.

3 For example,see: https://www.theguardian.com/world/2020/jan/23/pwc-growing-scrutiny-isabel-dos-santos-scandal-luanda-leaks-angola#maincontent.

9.11 There continues to be a risk that criminals will exploit company liquidation and associated services (including insolvency practice, which may be conducted by certain accountancy professionals) to mask the audit trail of money laundered through a company. Regulatory guidance, increased supervision and strict legislative requirements on ASPs go some way to mitigate the risks of providing these services.

9.12 As highlighted in the 2017 NRA, it is likely that criminals continue to try and use the client accounts of ASPs to move large amounts of criminal funds quickly. However, supervisors have strict rules and guidance on how their members should handle client money, which reduces the likelihood of this abuse. We consider that the risk of an ASP's client accounts being used to launder money is lower for those supervised by a PBS or HMRC, than those that are operating unregulated.

9.13 Some supervisors have expressed concern that while still rare, ASPs are being increasingly asked to accept payment in cryptoassets. While use of cryptoassets alone is not necessarily suspicious, cryptoassets can be used to disguise the origin of funds more easily than other payment methods.

Terrorist financing

9.14 The risk of terrorist financing through accountancy services is low. We continue to assess that accountancy services are not attractive for terrorist financing and there remains no evidence of these services being abused for terrorist financing purposes.Supervision, compliance and law enforcement response Supervision and compliance

9.15 The 2018 UK Mutual Evaluation Report by the Financial Action Task Force (FATF) highlighted the inconsistencies in the AML supervision of the accountancy sector and the need for improvement, while noting the recent formation of OPBAS. Similarly, the 2019 Economic Crime Plan acknowledges the work of OPBAS and includes an assigned action (Action 36) for OPBAS to continue to strengthen the consistency of professional body AML supervision.

9.16 Changes to the MLRs in 2017 have boosted supervisors' capability to tackle non-compliance in their sector and the creation of OPBAS in 2018 has provided the PBSs with expectations on supervisory standards and a means of actively monitoring them. Although HMRC does not fall under OPBAS's remit for ASP supervision, they have committed to align their supervisory approach4 to the standards of the OPBAS Sourcebook5 to further improve the consistency of ASP AML supervision.

9.17 Since the 2017 NRA, OPBAS has worked with the accountancy sector PBSs to increase the consistency of their AML supervision and facilitate increased intelligence and information sharing. OPBAS has assessed all 13 accountancy PBSs against its Sourcebook and is monitoring PBS action plans accordingly to address weaknesses identified. To further ensure consistency, OPBAS have held 4 workshops with the PBSs to cover areas of commonly identified weakness including: governance, risk-based approach, supervision and intelligence and information sharing.

9.18 In their 2020 supervisory report, OPBAS observed a notable increase in PBSs having appropriate governance arrangements for AML supervision; improvements in the application of a risk-based approach and an increase in PBSs undertaking proactive AML supervision. 6 The full impact of changes in AML supervision by the PBSs continues to be tested and assessed by OPBAS for effectiveness. This will be a focus of OPBAS supervision in 2020 to 2021.

9.19 Members of the Accountancy AML Supervisors Group (AASG) have continued to share good practice on the 'risk-based approach' required by the AML regime, ensuring a proportionate and consistent approach to different risk profiles while at the same time reflecting specific demographics of their membership, the services they provide, the nature of their clients and the geographic reach of member firms.

9.20 Intelligence and information sharing has also improved with OPBAS, alongside the National Economic Crime Centre (NECC), establishing the Intelligence Sharing Expert Working Groups (ISEWGs). The AASG members have also enhanced information and intelligence sharing, by actively engaging with OPBAS and the Accountancy ISEWG and in disseminating Joint Money Laundering Intelligence Taskforce (JMLIT) amber alerts.

9.21 This is alongside an increase in the number of self-reported AML related fines issued by ASP supervisors, with fines increasing to 226 in 2018 to 2019 up from 126 in 2017 to 2018.7 However, the average fine amount has decreased and this increase in the number of fines was not consistent across all 13 accountancy PBSs; 3 did

not issue any fines at all during the relevant period.

9.22 Likewise, wider public-private partnership work on private to private known suspicion information sharing will explore the feasibility of a mechanism to share information, both within and across sectors, on bad actors who have been exited or refused a service. This aims to improve the effectiveness of know your customer checks (KYC) and customer due diligence (CDD) processes at the point of taking on a client to reduce the number of customers firms are required to exit.

4 Action 35 in the UK's Economic Crime Plan.

5 'Sourcebook for professional body anti-money laundering supervisors', OPBAS, January 2018.

6 'Anti-Money Laundering Supervision by the Legal and Accountancy Professional Body Supervisors: Progress and themes from 2019', OPBAS, March 2020.

7 'Anti-money laundering and counter-terrorist financing: Supervision report 2018-19', HM Treasury, August 2020.

9.23 There have also been a number of roundtable sessions held with the Economic Secretary to the Treasury, John Glen, where PBS senior leaders have been recognised for their progress so far but where they were also reminded of the importance of OPBAS's work and that the government expects more to be done to tackle illicit finance in the professional services sector.

9.24 There are still variable levels of understanding of the AML risks in the sector by ASP firms and individuals, which may limit the effectiveness of mitigations. For example, criminals can evade the checks that could identify their suspicious activity if firms do not conduct appropriate risk-based controls. The key non-compliance trends ASP supervisors have identified are a lack of comprehensive risk assessments or appropriate risk-based controls and poor documentation or record keeping demonstrating appropriate client due diligence. The drivers behind this are:

- a failure by ASPs to understand their obligations under the MLRs, therefore making them more vulnerable to abuse if they are lacking robust AML compliance procedures.
- non-prioritisation of AML compliance responsibilities by ASPs looking to save time and costs, or compliance being approached in a tick box manner.
- the lack of accountancy specific AML training available to ASPs, along with the lack of time or funding for training.

9.25 Transparency of beneficial ownership has also long been viewed as an issue in the UK, due to the nature of the company formation process. In September 2020, the Department for Business, Energy & Industrial Strategy published a response to its consultation on options to enhance the role of Companies House, committing to take forward plans to increase transparency and introduce ID verification for individuals setting up, controlling and owning companies.8 The consultation has helped the government consider how we can improve the accuracy and searchability of the information held at Companies House, and give it greater powers to query and check the information submitted to it.

Law enforcement response

9.26 Steps have been taken to improve information sharing between law enforcement, supervisors and firms, which is increasing the collective understanding of the AML/CTF risks in the sector.

9.27 OPBAS, alongside the NECC and the JMLIT, established the ISEWGs in 2018 to 2019. The ISEWGs reflect the initial steps in sharing intelligence between PBSs, statutory AML supervisors and law enforcement. They were created to offer a platform for strategic and tactical intelligence to be shared and enable

communication between supervisors and law enforcement, and enable a greater understanding of the threat which supervisors can take account of in their supervisory activities. For the accountancy sector, all ASP supervisors are members of the ISEWG, including HMRC, as well as the NECC and the Financial Conduct Authority (FCA). There have been 6 strategic accountancy ISEWGs to date with a further 5 bilateral tactical intelligence sharing sessions taking place between individual accountancy PBSs and law enforcement.

8 'Corporate Transparency and Register Reform - Consultation on options to enhance the role of Companies House and increase the transparency of UK corporate entities', BEIS, September 2020.

9.28 Since the ISEWG's creation, OPBAS has seen a significant rise in intelligence centred communication between law enforcement, third parties and the PBSs. For example, up until March 2020, 32 detailed section 79 requests have been shared between the National Crime Agency and the accountancy PBSs relating to live investigations.10.

9.29 Outside the ISEWGs, the number of Suspicious Activity Reports (SARs) reported by accountants has seen a slight increase of 3.5% in 2019 to 2020, compared with the 2017 to 2018 period. The SARs guidance working group, including reporting sectors, the UK Financial Intelligence Unit (UKFIU), OPBAS and supervisors, is engaged with the sector on developing updated guidance. There is recognition that further work is required to improve effectiveness of the SARs reporting by the sector; improving the quality and effectiveness of information provided, as well as the percentage of ASPs who report SARs will help towards addressing this issue.

9.30 Targeting professional enablers is a priority for the NECC in its response to money laundering. The NECC has established a dedicated practitioners group to formulate a pipeline of cases for enforcement action. The Enablers Practitioners Group (EPG) also serves to inform best practice and share operational learning on professional enablers across the law enforcement community. Complex financial crime investigations can be hindered by the need to deploy specialist investigation skills, including forensic accountants, and the NECC has utilised the EPG to identify these resources across law enforcement and make them available to operational case teams.

Box 9.A: Case study 1

9.31 A PBS conducted an AML compliance review of a sole practitioner. The review started as a desk-based review. Upon receipt of the initial set of documents requested, the type and nature of clients of the firm raised some concerns with the reviewer. Open source research was conducted on the clients which raised further concerns as they identified a number of high-risk indicators of involvement of the client in human trafficking. Despite this, the sole practitioner had categorised

9 Section 7 of the Crime and Courts Act 2013 is an information sharing gateway between the NCA and others to share information to assist the NCAs function.
10 Anti-Money Laundering Supervision by the Legal and Accountancy Professional Body Supervisors: Progress and themes from 2019', OPBAS, March 2020.

all the clients as low risk for money laundering. At this point it was not clear if the sole practitioner was knowingly involved or had not identified these issues because of a lack of awareness and controls. An onsite visit was made to the sole practitioner to establish more about their procedures and risk assessment. The PBS also gathered more details on the clients (including the names, nationality, date of birth, National Insurance Numbers of the individuals working in the massage parlours as the firm provide payroll services so had these on file) which they included in a report to the UKFIU. Following the review, the PBS determined that the sole practitioner did not have an awareness of risk or the threats posed by his clients, and do not believe he was knowingly involved. No further action was taken.

Box 9.B: Case study 2

9.32 Through its risk-based approach to supervision, an accountancy sector PBS identified significant weaknesses in the AML compliance of a member.

9.33 The PBS's intelligence section identified concerning information linked to the staff/client ratio of the practice, which was being run as a one- man, sole trader operation. The firm was also acting as a TCSP, with research showing that there were tens of thousands of Companies House matches, of both companies and officers, registered at the premises. This was considered a substantial amount for a sole trader to manage.

9.35 The compliance inspection identified significant failures in the member's AML systems and controls, including a lack of understanding of AML risk and outdated policies and procedures. It also found that although client due diligence was outsourced to a third-party company, which was run by a relative of the practice licence holder, there was a total lack of acceptable CDD carried out by this practice. Open source research also discovered that a family member of the practice licence holder, who was also a haulage contractor client of the practice, had recently been convicted of serious criminal offences and sentenced to a lengthy period in custody.

9.36 Although they could not establish any links between the practice and the criminality uncovered, the PBS did find this information relevant in assessing the member's risk profile. Formal disciplinary action was then taken against the member.

Risks Relevant to companies, partnerships and trusts

Extract from National Risk Assessment 2020:

Chapter 11

Companies, partnerships and trusts

Company, partnership and trust risk scores

	2017 Risk Score	2020 Risk Score
Company and partnership risk scores		
Money laundering	High	High
Terrorist financing	Low	Low
Trusts Risk Scores		
Money laundering	Medium	High
Trusts Risk Scores		
Terrorist financing	Low	Low

Summary and risks

- The 2017 NRA highlighted that companies and trusts are known globally to be misused for money laundering, and as a global financial centre the UK is particularly exposed to criminal exploitation of these activities. There remains insufficient evidence to quantify the exact extent of money laundering through UK companies, partnerships and trusts, but the vast majority are assessed to be used for legitimate purposes.
- The possibilities to create complex structures and enhance anonymity makes a corporate structure an attractive tool for criminals, and their use is regularly identified within money laundering investigations. This may be supplemented with other services provided by Trust and company service providers (TCSPs), for example 'shelf' companies which provide banking and credit history, together with nominee shareholders or directors.
- We continue to assess that there is a high risk that UK companies and partnerships will be abused for money laundering. This is unchanged from the 2017 NRA. Changes since 2017 have targeted some of the vulnerabilities identified, for example by extending Persons of Significant Control (PSC) registration to Scottish limited partnerships (SLPs). Since then, the number of registrations of new SLPs has greatly reduced though it is unclear if this has reduced the use of SLPs overall, for either legitimate or illegitimate purposes. However, other vulnerabilities within the framework to establish and verify companies and partnerships persist, maintaining their attractiveness for money laundering. Planned reform will further improve the transparency and oversight of the UK framework.
- There is little evidence that trusts established within the UK are used for illicit purposes, but government is seeking to expand its knowledge base on trusts. It is too early to determine if the greater registration of trusts through the Trust Registration Service will generate greater intelligence. Overall, the risk of UK trusts being abused for money laundering is assessed to be low. This rating is unchanged from the 2017 NRA.
- TCSPs are not necessary for the abuse of legal entities and arrangements for illicit purposes, but they can assist in their exploitation, for example by creating the complex structures which impede investigations or obscure beneficial ownership. Since the last NRA, our understanding of the scale of TCSP use linked to money laundering and risk from them has increased greatly. Based on this, we now assess the money laundering risk from TCSPs as high.
- We have seen little evidence of exploitation of trusts, companies or partnerships for terrorist financing purposes. Therefore, the terrorist financing risk is assessed as low.

UK companies and partnerships

11.1 UK companies and partnerships continue to be at a high risk of being used for money laundering purposes. UK legal entities,1 such as limited companies, limited liability partnerships (LLPs) and SLPs are exploited to facilitate a range of illicit activity, including large scale money laundering and tax evasion. When PSC requirements were brought in for SLPs, there was a drastic reduction in the registration of them, with incorporations of SLPs falling from 4,932 in 2016 to 2017, to 2,689 in 2017 to 2018, and falling further to 657 in 2019 to 2020. Although England and Wales limited partnerships (EWLPs) and Northern Ireland limited partnerships (NILPs) do not offer a separate legal entity, unlike SLPs, there was a significant rise in registrations of these structures in 2017 to 2018, when PSC requirements were introduced for SLPs. Although, the total of new registrations was a fraction of the reduction in new SLPs.2 The number of incorporations of EWLPs and NILPs has since returned to pre-2017 to 2018 figures. While we have no firm evidence of abuse of EWLPs and NILPs, it is likely that some of this demand was driven by criminals seeking to exploit EWLPs and NILPs for illicit purposes. As of June 2020, there are now estimated to be over 4 million companies registered. The vast majority of these are used for legitimate purposes.

1 Legal entities include: public and private limited and unlimited companies, Scottish general partnerships, Scottish limited partnerships and (all) limited liability partnerships.

2 For England and Wales Limited Partnerships, 1,415 were registered in 2017-18 compared with 645 in 2016-17, with comparable figures for NILPs being 349 registration in 2017-18 compared with 73 in 2016-17.

11.2 Corporate structures are used globally for money laundering schemes, particularly where they offer opacity that can be exploited to conceal beneficial ownership. UK companies and partnerships are likely to be particularly attractive for money laundering due to the UK's international reputation for trade and finance and rule of law. While UK legal entities may be involved in money laundering schemes, and the legal entity can disguise the origin of the funds or make them appear legitimate, these funds do not necessarily flow through the UK. This means that due diligence typically sits in the jurisdiction where the transaction takes places, and UK authorities may not become aware of these transactions or accounts unless brought to their attention. Criminals benefit from the implied trustworthiness of the UK legal entity but are not necessarily subject to the same anti-money laundering and counter-terrorist financing (AML/CTF) checks as a company with an account held by a UK bank.

11.3 There are several factors that continue to make UK companies and partnerships vulnerable to being used for money laundering purposes. While the UK has reporting requirements in place for legal entities and arrangements, as well as a requirement for UK companies, LLPs and SLPs to provide information of their people with significant control to Companies House, there remains gaps that can be exploited to disguise beneficial ownership and control of entities and their assets. Creating complex, multi-layered structures can help keep beneficial owners anonymous, particularly if entities within the chain are based overseas in secrecy jurisdictions.

11.4 UK legal entities can be set up within a matter of hours, very cheaply, and with few barriers. If they are set-up directly with Companies House rather than through a TCSP, there is no requirement to go through AML/CTF checks. Furthermore, overseas TCSPs can form companies directly through Companies House and are included in the list of formation agents on the Companies House website. Entities have been found to breach national reporting requirements by falsely declaring themselves dormant or providing inaccurate identity information to Companies House, who are not in a position to know otherwise.

11.5 The Department for Business, Energy & Industrial Strategy (BEIS) and Companies House are taking steps to increase the transparency of companies and other legal entities through Limited Partnership Reform and Corporate Transparency and Register Reform programmes. See paragraphs 11.30 to 11.32 below for more details.

11.6 It is difficult to ascertain the extent to which different legal entities and arrangements are used to facilitate money laundering. There is strong evidence of UK limited companies, LLPs and SLPs being abused to facilitate the laundering of millions of pounds. For example, in BEIS' 2018 consultation on Limited Partnership Reform, it was noted that the National Crime Agency (NCA) has identified a disproportionately high volume of suspected criminal activity involving Scottish limited partnerships, and there have been prominent examples of them featuring in international money laundering schemes that have made international headlines.3 While there is

3 'Limited Partnerships: Reform of limited partnership law.', BEIS, April 2018.

less evidence of the abuse of EWLPs and NILPs and they do not offer the separate legal entity granted by SLPs, there is a possibility that they could still be used within opaque corporate structures, or used in overseas jurisdictions where their legal status may not be properly understood. It is likely that these structures are attractive for money laundering purposes due to the lower reporting requirements on those that ultimately control the partnerships, compared with legal entities. For example, registrations

for NILPs increased by 582% in 2017 after the requirement for PSC information on SLPs was introduced, though the number of registrations has since fallen back to pre-2017 levels. The Government has announced plans to modernise limited partnership law, which would improve the transparency of these kinds of structures and make them easier to understand (see paragraph 11.31 below).

11.7 The lack of evidence of UK companies and partnerships being used for terrorist financing means the risk is still assessed to be low.

Trusts

11.8 The misuse of trusts for money laundering remains a global problem, particularly in the role they play in the layering of funds. They can be used (often alongside corporate entities) to create complex structures which increase the difficulty of identifying if they are being used for illicit purposes or investigating illicit funds held within, and can provide anonymity to individuals, slowing down investigations and protecting the proceeds of crime. However, trust arrangements are often more complicated to establish than companies or partnerships, with a different legal status and utility, and are more likely to require professional support to establish. The transfer of control of assets may also make them unattractive to some criminals. Due to these factors, and the limited evidence of UK trusts being used for illicit purposes, the money laundering and terrorist financing risk for UK trusts is assessed as low.

11.9 Within the UK, law enforcement agencies rarely encounter abuse of UK trusts in high-end money laundering investigations. Overseas trusts are likely to be more attractive for illicit purposes as they can offer better levels of secrecy and tax advantages compared to UK-based trusts, while removing funds beyond the UK's AML/CTF regime and the investigatory powers of UK law enforcement.

11.10 Trusts are established for a range of legitimate purposes. These include but are not limited to: managing assets on behalf of vulnerable persons, including children; jointly holding property; ensuring inheritance is distributed in accordance with a person's last will and testament; performing commercial activity; and conducting charitable work. Each type of trust has different levels of utility, restrictions and requirements, meaning that they all carry different levels of risk.

11.11 The 2017 Money Laundering Regulations (MLRs) legislated for a UK central registry of trusts with tax consequences, maintained by HM Revenue & Customs (HMRC). This Trust Registration Service had 107,500 registrations as of 5 March 2019. This excludes a significant volume of trusts, including bare trusts which do not generate tax consequences to trustees. The transposition of the EU's Fifth Money Laundering Directive (5MLD) broadened the scope of the trusts register, but given the low evidence base for the use of UK trusts in money laundering, the effect on money laundering risk is uncertain.

11.12 Where trusts are abused by UK-linked criminals, they are almost invariably administered offshore, including in several Unexplained Wealth Order cases managed by the NCA.

11.13 The introduction of beneficial ownership registers for corporate entities in several overseas jurisdictions may make them less attractive for money laundering purposes overall, but these registers do not apply to trusts, so they will likely remain attractive for criminal purposes. It is also possible that other jurisdictions which have not introduced registers for beneficial ownership will become increasingly popular destinations for criminals and corrupt elites to deposit their illicit proceeds.

Trust and company service providers (TCSPs)

11.14 TCSPs can be exploited, either wittingly or unwittingly to enable the laundering of significant illicit flows through companies, partnerships and trusts. They often offer services which can enhance the attractiveness of

companies and partnerships to criminals, for example increasing anonymity or creating complex structures. While it is assessed that the majority of UK TCSPs adequately risk assess their clients and seek to understand the nature of their customer's business activity, it is almost certain that a relatively small number do not fully understand the risks involved. Evidence has demonstrated the laundering of millions of pounds through UK legal entities established by TCSPs. The risk of TCSPs being used to facilitate money laundering is therefore rated high.

11.15 Although UK companies and partnerships can be set-up directly with Companies House with comparative ease and low cost, approximately half of corporate entities are still established through TCSPs. TCSPs offer a convenient method to establish a company for legal purposes, but many of their services can be exploited by criminals, including the use of nominee directorships, UK mail forwarding services and providing a registration address for hundreds of companies at single addresses. This is particularly attractive for those establishing a UK company from overseas, since the company must have a UK registered office to serve as its official address but is not required to operate in the UK or have a UK bank account.

11.16 Other services can enhance the vulnerabilities of companies, partnerships and trusts discussed above. For example, TCSPs often sell 'shelf' companies; these are reputable companies with established banking and credit histories or nominee shareholders and directors. These are attractive to criminals because once purchased, the criminal can more easily hide their money laundering behind the reputable history and further conceal true ownership information.

11.17 The provision of nominee shareholders and directors by some TCSPs can also be high-risk. This is particularly the case where TCSPs offer directors where the directors have no understanding of the business and no oversight of its operations, or where they offer directors who are already the director for 20 or more companies.

11.18 It is likely that a high proportion of high-risk TCSPs are in the minority of stand-alone TCSPs supervised by HMRC. These include specialist company formation agents and virtual office providers, which are often skilled in the layering of corporate structures and use of anonymity provisions to clients. There are about 23,400 UK registered businesses that provide TCSP-related services and 24 different UK TCSP supervisors. For most, TCSP activity is not the firm's core business activity; this is usually another supervised activity such as accountancy (approximately 16,800) or legal services (approximately 5,400) but can include non-supervised activity, such as management consultancy. In such cases, the TCSP activity is usually carried out on top of other work regulated by its Professional Body Supervisor (PBS). Such companies can combine TCSP services with other professional services such as legal or accountancy provision. The interlinking of TCSP services with other professional services is at high risk of being used to create complex legal structures. See chapter 9 on accountancy service providers and chapter 10 on legal service providers for more detail on the risks in these sectors.

11.19 There appears to have been significant consolidation in the TCSP sector, with the number of HMRC-supervised TCSPs declining from 2,640 in 2014-15 to 1,366 in 2018 to 2019. Over half of all company incorporations in 2018 to 2019 were undertaken electronically by just 106 companies, many of whom are TCSPs. The high level of competition in the TCSP sector likely creates additional risks, for example companies often attract customers by offering the rapid incorporation of companies. Systems are available to conduct rapid customer due diligence (CDD), but it is likely that such services are at increased risk of attempted criminal exploitation. The sale of shelf companies is often also advertised as a time-saving benefit, but they can also serve illicit purposes by creating a false impression of longevity.

11.20 UK TCSPs can provide services directly to overseas TCSPs. Overseas TCSPs are not subject to the UK MLRs, and beyond the European Economic Area, they are subject to varying levels of regulation. This increases

the risk to UK-based TCSPs due to low CDD carried out by overseas TCSPs. TCSPs are also sometimes unsure of the authenticity of identity documents presented during the CDD process, with several examples identified by HMRC where individuals were unwilling to provide identity documents.

Terrorist financing

11.21 The risk of terrorist financing through trusts, companies or partnerships is low. We continue to assess that these are not attractive for terrorist financing and there remains no evidence of them being abused for terrorist financing purposes.

Supervision, compliance and law enforcement response

Compliance and supervision

11.22 As has been discussed earlier in this chapter, high levels of competition in the TCSP sector likely creates vulnerabilities through the need to provide rapid registration services to customers, and the potential for poor CDD this implies. The lack of resources available for CDD, training and AML decision-making in smaller TCSPs exacerbates this problem. Non-compliant TCSPs will often use generic policies, controls and procedures not tailored to their business or specific customer patterns.

11.23 It is possible for a TCSP to have complied with the MLRs but still have been utilised for illicit purposes for example, because it was provided with false CDD information which it failed to detect. It is also possible for a complicit business to present a facade of apparent compliance.

11.24 Due to the range of possible professional service providers which may undertake TCSP activity, the supervision regime remains diverse. This includes the Financial Conduct Authority (where it supervises entities for other purposes), the 22 PBSs for legal and accountancy service providers, who are supervised by Office for Professional Body Anti-Money Laundering Supervision (OPBAS), and HMRC. HMRC hosts a TCSP register populated by the PBSs and can supply information from the register to law enforcement agencies on request. PBSs are required to notify HMRC if members report undertaking TCSP activity, so the register can also help identify non-supervised TCSPs. The public portal allowing users to verify HMRC businesses includes all HMRC supervised TCSPs.

11.25 OPBAS seeks to strengthen the supervisory regime and ensure that the 22 PBSs provide consistently high standards of supervision. OPBAS also have an assigned action under the Economic Crime Plan to increase the consistency of PBS AML supervision. Since being established in 2018, OPBAS has taken steps to increase the consistency of PBS AML supervision including issuing each PBS with a findings letter outlining their weaknesses, monitoring PBSs implementation of improvements and holding additional workshops to outline expectations and share good practice. OPBAS will continue to assess the effectiveness of PBS AML supervision, including TCSPs, in 2020 to 2021.

11.26 The 2020 OPBAS report outlined improvements in the approach of PBSs to AML supervision. PBSs are also renewing their focus of TCSP supervision utilising tools such as thematic reviews to assess their populations and target their supervisory approach at high-risk areas.

11.27 Most PBSs report having adequate powers to deal with MLR breaches among their supervised populations. Action by PBSs against breaches of the MLRs has however been rare, with most preferring to use disciplinary powers in relation to professional standards breaches, and only one example could be found of where a PBS had revoked membership due a breach of the MLRs.

11.28 More robust supervisory action against UK TCSPs must be alongside the reforms to Companies House

outlined below, to ensure that greater supervisory action does not just displace the risk, either to overseas TCSPs or to criminal groups directly setting up their own UK companies and partnerships.

Policy changes

11.29 The Persons of Significant Control register was expanded in June 2017, requiring SLPs to file their beneficial ownership information. We are unable to determine what impact this has had on the abuse of legal entities and arrangements for money laundering purposes. Gaps remain that enable UK legal entities and arrangements to be abused for money laundering, including the establishment of PSCs outside of the UK beyond the reach of UK law enforcement, limited data quality and validation checks, and poor CDD checks by some TCSPs.

11.30 BEIS' Corporate Transparency and Register Reform programme and their Limited Partnership reform programme will address many of these vulnerabilities. Newly announced proposals for Corporate Transparency and Register Reform will improve the accuracy and usability of the data on the companies register, helping us know who is setting up, managing and controlling corporate entities. Greater legal powers to query and seek corroboration on information submitted, closer work with law enforcement and other partners to support investigations and an improved analytical capability will help to detect suspicious activity earlier and hold those responsible to account.4

11.31 BEIS published their response to their Limited Partnership reform consultation in December 2018 and are now working to implement their proposed measures. This will include further work to explore whether to require beneficial ownership information from corporate partners that do not already hold a PSC register. This will take into account the value to law enforcement of this information; their relevance to the UK's compliance with international standards; the existing reporting requirements of these entities; and the potential burden of introducing these reporting requirements.5 Further potential reform includes making it mandatory for presenters of new applications for registration of limited partnerships to demonstrate that they are registered with an AML supervisory body, and to provide evidence of this on the application form, more stringent requirements on demonstrable links to the UK, greater reporting requirements and greater powers for the Registrar to strike off limited partnerships that are now dissolved or which the Registrar concludes are not carrying on business or in operation. These will all serve to reduce the opportunities to misuse limited partnerships and improve the quality of information of the register.

11.32 The introduction of discrepancy reporting in January 2020 as part of 5MLD, is also improving the quality of beneficial ownership data held on the PSC register. Obliged entities are required to notify Companies House when it identifies a discrepancy between the information it holds and that held by Companies House. As of August 2020, there had been over 3,000 reports submitted so far.

4 'Corporate Transparency and Register Reform Government response to the consultation on options to enhance the role of Companies House and increase the transparency of UK corporate entities', BEIS, September 2020.

5 'Limited Partnerships: Reform of Limited Partnership Law. The Government response to the consultation.', BEIS, December 2018.

11.33 The UK has also expanded the trusts register as per 5MLD to require registration of UK express trusts and 2 further sorts of trusts.6 It is too early to ascertain how the information provided by greater registration will assist law enforcement agencies and other authorities in tackling the misuse of trusts.

11.34 There is ongoing work to improve the capability of law enforcement agencies in tackling the threat posed by overseas trusts. The 2017 NRA noted that every Crown Dependency and Overseas Territory with a financial centre had signed up to the Common Reporting Standards (CRS), the new global standard for tax transparency,

under which CDOTs will share details of financial accounts (including trusts) which are held in their countries and belong to UK tax payers with HMRC.

11.35 Most CDOTs with financial centres have also developed private central registers of corporate beneficial ownership. Information in these registers are accessible to UK law enforcement agencies through bilateral arrangements. These arrangements were assessed in a UK Statutory Review, which was published in June 2019, and found to be providing highly effective support to UK law enforcement investigations. Access to this information has enabled the seizure of illicit funds, including a case with an approximate value of £25 million. See paragraphs 4.32 - 4.38 for more details on the risks associated with CDOTs.

Law enforcement response

11.36 The 2017 NRA drew attention to the low levels of Suspicious Activity Reports (SARs) submitted by TCSPs since the 2015 to2016 reporting period. This downward trend continued with the sector seeing a 41.5% decrease in reporting for the period 2019 to 2020 compared to the 2017 to 2018 period. However, the trend partially reversed this year, with the UK Financial Intelligence Unit (UKFIU) reporting a 34.78% increase for 2019 to 2020, compared to the 2018 to 2019 period.7 It is accepted that TCSPs may also be reporting SARs as either legal or accountancy service providers. The decline in SARs is also likely due in part to the drop in number of TCSPs who identify as a TCSP rather than being part of the accountancy or legal sectors. However, the level of reporting may also be due to a lack of awareness

6 UK express trusts with taxable consequences are already required to collect information on beneficial ownership and register with HMRC's Trust Registration Service (TRS). New regulation 45ZA now widens the scope of trusts required to register to include all UK express trusts, including those with no tax consequences, with explicit exemptions for some categories of trusts. Non-UK trusts are also required to register where the trust has at least one UK resident trustee and enters into a UK business relationship, or where the trust acquires an interest in land in the UK.

7 The significant percentage fluctuations between reporting periods should be viewed in the context of the low number of SARs reported in this sector each year. Suspicious Activity Reports (SARs) Annual Report 2018', NCA, November 2018, and 'Suspicious Activity Reports (SARs) Annual Report 2020', NCA, November 2020; Suspicious Activity Report (SARs) Annual Report 2019, NCA, November 2019 among reporters, a lack of resources needed to submit reports, or the lack of penalties for not doing so.

11.37 The National Economic Crime Centre (NECC), working with law enforcement partners including HMRC, has developed a plan to address the illicit finance risks associated with the TCSP sector. The NECC is identifying those TCSPs which represent the highest risk to the UK, and is tasking supervisory and/or law enforcement bodies to take appropriate action against them. The NECC is also improving the law enforcement intelligence picture in relation to TCSPs. This enriched intelligence picture has also been used to inform the government's corporate transparency reforms. For example, it has allowed the NECC to identify core vulnerabilities within the current corporate transparency framework relating to the TCSP sector, and the NECC has engaged with BEIS on behalf of its partner agencies to share their views in the Corporate Transparency and Register Reform consultation.

Box 11.A: Abuse of overseas trusts

11.38 A business owner who avoided tax by under declaring profits from his business laundered the funds by using a trust based in Gibraltar. The trust was set up and money transferred to the trust from bank accounts in the UK, with the assistance of a complicit accountant. The beneficiary was recorded as his daughter, and funds were transferred to bank accounts in Cyprus believed to have belonged to his daughter, but the money was later used to purchase property for the business owner.

Box 11.B: UK-based TCSPs providing services to overseas TCSPs

11.39 A UK based TCSP provided LLP, SLP and other legal entities to 2 non- UK based TCSPs (one based in Latvia, one in Cyprus). The UK-based TCSP considered the overseas TCSPs the customers, had met them and assessed them as low risk. The UK TCSP did not raise suspicions when products used to favour anonymity were requested and failed to monitor suspicious patterns of behaviour (for example, after legislative changes introduced a requirement for one director of a company be a natural person, the intermediaries requested SLP/LLP arrangements instead).

Risk Assessments

Summa Accountancy Services Limited uses risk assessments to help direct its resources to the areas and clients that present the highest risk to the Firm of ML/TF. This is part of the Risk Based Approach adopted by Summa Accountancy Services Limited, an approach which is endorsed by the UK AML/CTF legislation and guidance.

The risk assessments will influence the level of Customer Due Diligence required by Summa Accountancy Services Limited.

Firm Risk Assessment

Summa Accountancy Services Limited is aware of both its obligation to undertake a Firm Risk Assessment under R.18 MLR2017 and the value of undertaking such a Risk Assessment.

Summa Accountancy Services Limited is conscious of how its own approach to risk and AML/CTF compliance will have an impact on Summa Accountancy Services Limited's own AML/CTF Risk Assessment. Key decisions that the firm has, or will make in the future regarding matters such as which sectors of clients to advise, the clients geographic location or whether to meet all clients will have an impact on the firm’s risk exposure to money laundering and terrorist financing. The firm’s appetite for risk is also a key factor.

Summa Accountancy Services Limited will consider the risks associated with the sector within which it operates and those that are connected to Summa Accountancy Services Limited's size and nature of operations.

Summa Accountancy Services Limited will review, update and communicate any consequential amendments of its firm risk assessment to its staff and senior management on an on-going basis.

Sector

Summa Accountancy Services Limited is aware of the need to review, discuss and amend its Firm Risk Assessment in accordance with guidance issued that is relevant to its sector. Such guidance may be issued by, amongst others, Summa Accountancy Services Limited's Anti Money Laundering Supervisor, other UK AML Supervisors, The UK Government, FATF (Financial Action Task Force) guidance and HM Treasury and Home Office.

Summa Accountancy Services Limited is also aware of the AMLGAS (Anti-Money Laundering Guidance for the Accountancy Sector) which is the only HM Treasury approved guidance for the sector and the PCRT

(Professional Conduct in Relation to Taxation).

Summa Accountancy Services Limited has specifically addressed the issues relevant to its sector raised and discussed within the latest UK National Risk Assessments of Money Laundering and Terrorist Financing and will review its Firm Risk Assessment in the light of subsequent National Risk Assessments.

The Firm as an Accountancy Service Provider

Summa Accountancy Services Limited is not knowingly involved in any ML/TF activities. Summa Accountancy Services Limited is therefore not complicit with ML/TF.

Summa Accountancy Services Limited does not work in collusion with any other element of the regulated sector or the unregulated sector to undertake ML/TF activities.

Summa Accountancy Services Limited is alive to the risk of being coerced into assisting with ML/TF by criminals.

Summa Accountancy Services Limited is conscious that criminals may seek to use Summa Accountancy Services Limited' skills and knowledge to distance the proceeds of crime from the beneficiaries of such proceeds by creating structures and vehicles that may disguise beneficial ownership of such structures and vehicles.

Summa Accountancy Services Limited is aware that criminals may wish to use Summa Accountancy Services Limited's services to try to add legitimacy to financial accounts or financial affairs of a person, entity or business in that those accounts could be used for criminal conduct.

The risk that Summa Accountancy Services Limited could not only add legitimacy through preparation of financial accounts but also by providing audit and assurance services.

Summa Accountancy Services Limited is alive to the risk of punishment if it does not report a matter to the National Crime Agency (NCA) that it is legally obliged to report.

This Summa Accountancy Services Limited is aware that it undertakes regulated work under the money laundering regulations and, as such, is required to be registered with a relevant AML supervisor.

Mitigation Steps

Summa Accountancy Services Limited adheres to its AML/CTF policy and procedures closely to ensure that it does all that it is able to do to prevent and detect ML/TF. Systems and controls are applied to confirm that Summa Accountancy Services Limited does comply with its policies and procedures. Monitoring of its own adherence to these policies and procedures and reporting to the MLRO (Money Laundering Reporting Officer) of any variation from these policies and procedures will minimise the risk that Summa Accountancy Services Limited is complicit in ML/TF.

Summa Accountancy Services Limited carefully chooses any other service providers within the regulated sector that it works with. It does this by identifying and verifying the professional qualifications and authority to carry out such services, of such service providers with any relevant regulators, register holders or professional bodies.

Summa Accountancy Services Limited is careful to keep relations with third-party regulated service providers transparent and not to make undisclosed agreements that if discovered could suggest inappropriate collusion between firms. Identification of such a collusion would be reported to Summa Accountancy Services Limited's MLRO.

Summa Accountancy Services Limited keeps a record of any improper comments or conduct by clients that might suggest that such conduct is an inducement or pressure to undertake a certain course of action that would be contrary to Summa Accountancy Services Limited's AML/CTF policy and procedures. Such conduct or comments will be reported to Summa Accountancy Services Limited's MLRO.

Summa Accountancy Services Limited is clear that it needs to follow its own AML/CTF policy and procedures, to minimise the risk that its services are used to create structures and vehicles that may aid ML/TF. Any suspicion of such activity will be reported to Summa Accountancy Services Limited's MLRO.

Summa Accountancy Services Limited takes an approach of seeking to review as much original third-party information as possible when producing a set of accounts for a client. Any transactions that raise a suspicion of ML/TF will be reported to Summa Accountancy Services Limited's MLRO.

Summa Accountancy Services Limited is conscious of its obligations under POCA (Proceeds of Crime Act 2002) and TACT (Terrorism Act 2000) with regards to making SAR (Suspicious Activity Reports) to the NCA (National Crime Agency). Summa Accountancy Services Limited believes that by following Summa Accountancy Services Limited's AML/CTF policy, procedures and controls will minimise the risk that a matter that should be the subject of a SAR to the NCA is not identified.

The Firm as a Trust or Company Service Provider

Summa Accountancy Services Limited undertakes some of the following work for clients that are classified as TCSP as follows:

(a) forming companies or other legal persons

(b) acting or arranging for another person to act

(i) as a director or secretary of a company, or

(ii) as a partner of a partnership, or

(iii) in a similar position in relation to other legal persons (see para 3.2.1)

(c) providing a registered office, business address, correspondence or administrative address or other related services for a company, partnership or any other legal person or arrangement

(d) acting or arranging (see para 3.2.2) for another person to act as

(i) a trustee of an express trust (see para 3.2.4) or similar legal arrangement, or

(ii) a nominee shareholder for another person other than a company listed on a regulated market which is subject to disclosure requirements consistent with Community legislation or equivalent international standards.

Summa Accountancy Services Limited is conscious of the overall approach to AML/CTF is crucial to having controls in place to prevent the misuse of its services by criminals.

Summa Accountancy Services Limited is not complicit in assisting criminals and has safeguards in place to minimise the risk of being used to negligently assist criminals.

Summa Accountancy Services Limited understands that criminals may wish to try to use its services for money laundering. This policy includes a review of the risks associated with the types of services that Summa Accountancy Services Limited offers.

Summa Accountancy Services Limited undertakes an individual risk assessment on every client that Summa Accountancy Services Limited works with to assess the risks of ML/TF associated with that client.

Summa Accountancy Services Limited is mindful that it has a duty to both seek to prevent and identify the use of its services for money laundering or terrorist financing.

Sector

Summa Accountancy Services Limited is conscious that by providing TCSP services it may be making itself attractive to criminals who may be looking to disguise the origin of proceeds of crime or who may be looking to move those proceeds outside of the UK.

Mitigation

Summa Accountancy Services Limited is not complicit in assisting clients to disguise ownership of corporate vehicles or to provide further layers of anonymity through the services that it provides.

Summa Accountancy Services Limited performs a detailed risk assessment on every client that it acts for both before making a decision to take a client on as well as an on-going process while a client continues to retain Summa Accountancy Services Limited's services.

Summa Accountancy Services Limited takes steps to mitigate the risks identified in a client risk assessment and if it feels that these risks cannot be sufficiently mitigated the client is disengaged.

Client Risk Assessment

Summa Accountancy Services Limited understands the importance of identifying and assessing the risk of a client being involved in ML/TF. In order for Summa Accountancy Services Limited to assess this, it is crucially important that it understands every client.

Summa Accountancy Services Limited is aware of guidance set out in r.18 MLR 2017 on its duty to identify and assess the risks of that its business is subject to. The Firm's own risk assessment will need to be extended by the need to identify and assess the risks of ML/TF associated with each of its clients. Any high-risk clients will require the firm to undertake its Enhanced Due Diligence policy and procedures.

Summa Accountancy Services Limited undertakes a detailed Client Risk Assessment using the AMLCC online risk assessment tool.

Such risk assessments are updated every year or as soon as circumstances change.

Summa Accountancy Services Limited considers its own Firm Risk Assessment when considering the risk level

associated with every client.

The level of the risk posed of ML/TF by each client will also drive the extent of Customer Due Diligence work undertaken on the client and will dictate if the Firm needs to follow its Enhanced Due Diligence policies and procedures. The risk assessment of a client that leads to a high risk outcome will lead to the Firm undertaking its Enhanced Due Diligence policies and procedures.

The Firm's client risk assessments must cover as a minimum:

- Customer risk factors
- Product, service, transaction or delivery channel risk factors
- Geographical risk factors

Customer Due Diligence

Customer Due Diligence (CDD): Introduction

Summa Accountancy Services Limited understands the influence that the risk assessment for ML/TF undertaken for every client has upon the level of CDD and on-going monitoring undertaken on that client.

Summa Accountancy Services Limited understands the need to both identify and verify all Beneficial Owners of every client who fall within the requirements of R.5 and R.6 of MLR 2017 which explains who is a beneficial owner, the Firm also understands the requirement to identify and verify clients who are not corporate clients. Summa Accountancy Services Limited is further aware of the requirement to identify, verify and confirm the authority to act for anyone who purports to act on behalf of a client.

Summa Accountancy Services Limited will also carry out CDD in accordance with R.27,28 and 29 MLR 2017 being mindful that the identification and verification of clients is part of Summa Accountancy Services Limited's CDD and not the full extent of it. Summa Accountancy Services Limited understands that it needs to know the type of business and the transactions the client is likely to undertake along with the expected nature and volume of transactions.

The firm is conscious of the guidance of when and how to perform CDD as set out within the online client and firm risk assessments in AMLCC.

Summa Accountancy Services Limited is mindful of r.28(18) which explains what verify means in the contact of CDD.

- Verify means on the basis of documents or information either obtained from a reliable source which is independent of the individual whose identity is being verified.
- Documents issued or made available to by an official body are to be regarded as independent even if provided or made available to the Firm by or on behalf of that person.

The firm is aware of the requirement from the 2020 amendments to the regulations to report discrepancies in beneficial ownership information to the relevant register.The firm is also aware that The Money Laundering and Terrorist Financing (Amendment) (EU Exit) Regulations 2020 amended this requirement to apply only when establishing a business relationship. R.30A(2)(b) of the ML regulations has been amended to reflect this.

Ultimate Beneficial Owners

Summa Accountancy Services Limited understands the importance of being clear on who the Ultimate Beneficial Owner(s) (UBO) is of every corporate client that it works with. Summa Accountancy Services

Limited is clear that the UBO of a body corporate may not be the legal owner recorded on the company's records or on the relevant national company registers.

FAFT (Financial Action Task Force) Recommendations (June 2017 update) refers in its glossary to a Beneficial Owner as:

Beneficial owner refers to the natural person(s) who ultimately (Reference to "ultimately owns or controls" and "ultimate effective control" refer to situations in which ownership/control is exercised through a chain of ownership or by means of control other than direct control.) owns or controls a customer (This definition should also apply to a beneficial owner of a beneficiary under a life or other investment linked insurance policy.) and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement

R.5 MLR 2017 includes an individual who exercises ultimate control over the management of the body corporate. It is noted that the introduction of "ultimate" is a change from the MLR 2007.

The firm is aware that The Money Laundering and Terrorist Financing (Amendment) (EU Exit) Regulations 2020 amended the requirement to undertake some aspects of CDD on a company listed on a regulated market (as defined in the ML regulations). R.28(5) of the ML regulations no longer requires the following for a company listed on a regulated market: Where the customer is a body corporate

a) the relevant person must obtain and verify

i) the name of the body corporate;

ii) its company number or other registration number;

iii) the address of its registered office, and if different, its principal place of business;

Summa Accountancy Services Limited is committed to taking all steps to identify and verify the UBO of its clients which are corporate bodies.

R.28(7) and (8) confirms the importance that the Firm has exhausted all possible means of identifying the beneficial owner of a body corporate. If after exhausting all possible means the firm has not succeeded in identifying the beneficial owner or is not satisfied that the individual identified is in fact the beneficial owner, then: The firm may treat the senior person responsible for managing the body corporate as the beneficial owner.

The firm understands the need to record in writing all of the actions it has taken to identify the beneficial owner where it has chosen to rely on R.28(7) & (8). This relates to a situation where the firm has been unable to identify a beneficial owner(s) of a client. The 2020 amendments to the regulations confirm that documentation is essential and what information is required.

The FAFT Guidance On Transparency and Beneficial Ownership (October 2014) offers the example (9) of formal nominee shareholders and directors as a method of obscuring beneficial ownership information. The FATF guidance goes on to explain the risks of not being clear of who the ultimate beneficial owners of a corporate body are.

Purpose and Intended Nature

Summa Accountancy Services Limited also understands the needs to obtain information on the purpose and intended nature of the business relationship or occasional transaction with a client. This is of equal importance to other parts of CDD duties.

Client Not Met Face to Face

Summa Accountancy Services Limited is aware of the additional difficulty that arises in identifying and verifying a client that has not been met face-to-face.

Summa Accountancy Services Limited is clear that having documents certified by a person of good standing is a key part of the identification and verification procedures.

Summa Accountancy Services Limited will seek to use electronic signatures, where possible, to help manage the associated increased risk of working with a client that Summa Accountancy Services Limited has not met.

The firm is aware that the 2020 regulation amendments now treat an Electronic Verification Process as being independent of the person that is being verified. The firm is aware that before solely relying on the Electronic Verification Process that it must be clear that the process is capable of providing an assurance that a person claiming an identity is, in fact, that person.

The firm is aware that The EU Exit provisions made under The Sanctions (EU Exit) (Miscellaneous Amendments) Regulations 2020 have updated 2017 ML regulations R.19(b) by replacing the "appropriate level of assurance..." with "assurance that the person claiming a particular identity is in fact the person with that identity, to a degree that is necessary for effectively managing and mitigating any risks of money laundering and terrorist financing". This amendment is reflected in the draft updated AMLGAS.

Enhanced Due Diligence (EDD)

Summa Accountancy Services Limited is particularly conscious of the need to undertake Enhanced Due Diligence (EDD) steps and monitoring in the circumstances where the client risk assessment dictates. Summa Accountancy Services Limited uses R.33 MLR 2017 as part of its role in establishing when EDD is required and is mindful of R.33(4) and (5) when considering what steps to take to perform its EDD and to establish the appropriate on-going monitoring.

Summa Accountancy Services Limited will not take on a high-risk client without undertaking EDD and being satisfied that the client is not involved in ML/TF.

Summa Accountancy Services Limitedis clear that the following measures should be included within its EDD R.33(4) and (5) MLR 2017:

- Examining the background and purpose of the transaction; so far as reasonably possible
- Increasing the degree and nature of monitoring of the business relationship to determine if the relationship is suspicious

The firm's EDD may also include:

- Seeking additional independent, reliable sources to verify information provided or made available to the Firm
- Additional measures to understand better the background, ownership and financial situation of the customers, and other parties to the transaction
- Taking further steps to be satisfied that the transaction is consistent with the purpose and intended nature

of the business relationship;
- Increasing the monitoring of the business relationship, including greater scrutiny of transactions

The 2020 regulations amendment now mean that where a client is established in high-risk third country that additional EDD is required as follows R.33(3)(A)MLR:

- obtaining additional information on the customer and on the customer's beneficial owner;
- obtaining additional information on the intended nature of the business relationship;
- obtaining information on the source of funds and source of wealth of the customer and of the customer's beneficial owner;
- obtaining information on the reasons for the transactions;
- obtaining the approval of senior management for establishing or continuing the business relationship;
- conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination.
- AMLGAS explains that in a situation where either the client or another party to a transaction is established in a high risk third country that the need for EDD is most likely to apply to services other than accountancy, but highlights handling client money or client assets as situations where it would apply.

Changes to Clients Identification and Verification Documents

Summa Accountancy Services Limited will seek updated documents from clients when the client details change or when documents held become out of date.

The firm is aware that the 2020 regulation amendments have introduced changes to the requirements to update CDD measures on a client. If the firm has a legal duty to contact a client during a year, with a view to reviewing information relevant to the firm's risk assessment of the client and which relates to the beneficial ownership of the client, then the firm must apply its CDD measures to the client, then the firm must apply its CDD measures to the client. Thus keeping CDD measures up to date on a client as updated information is identified.

Use of Online Electronic Verifications

Summa Accountancy Services Limited is aware of the availability of Online Electronic Verifications (referred to in the regulations as Electronic Identification Process) which can be purchased to assist with verification of a client's identification.

Summa Accountancy Services Limited recognises that unless such verifications include biometric identification factors then sight of original or suitably certified independent and reliable photo ID will be sought alongside any electronic verifications used. This is to address the risk that the person claiming an identity may not be that person.

Online Verification Searches

Summa Accountancy Services Limited will use searches using reputable online search engines to help with gathering information on clients. This may be useful in a number of areas including identification of PEPs, understanding what work a client undertakes and considering any media comment in relation to the client.

Summa Accountancy Services Limited may use such information or update services as part of its on-going client monitoring. Summa Accountancy Services Limited may use google alerts as part of its monitoring of clients.

The firm is aware of the requirement to address the risk that a person claiming an identity is not that person and

that online verification search, if it to be relied on solely, must be capable of addressing that risk.

Politically Exposed Persons

Summa Accountancy Services Limited is aware of its obligations to have systems and procedures in place to determine if a client or its beneficial owner is a PEP or a family member or close associate of a PEP.

Summa Accountancy Services Limited is aware of the definition of a PEP within R.35(12) and (14) of MLR 2017 which defines a PEP. R.35 MLR 2017 is also considered in relation to what EDD step to undertake if a PEP is planned to be taken on as a client of Summa Accountancy Services Limited.

Summa Accountancy Services Limited is also conscious of guidance within R.36 of MLR 2017 and guidance on PEPs issued by the FCA.

https://www.fca.org.uk/publication/finalised-guidance/fg17-06.pdf

Summa Accountancy Services Limited will not accept a PEP as a client without senior management approval.

Timing of Verification

R.27(1) sets out the when the Firm should apply due diligence measures. These are:

- When the Firm establishes a business relationship (which is further defined in R.4 MLR 2017)
- When the Firm carries out an occasional transaction that exceeds 1,000 euros and amounts to a transfer of funds under Article 3.9 of the funds' transfer regulation
- When the Firm suspects ML/TF
- When the Firm doubts the veracity or adequacy of documents or information previously obtained for the purposes of identification and verification.

Summa Accountancy Services Limited is conscious of R.30 MLR 2017 which relates to the timing of identification and verification when taking on a new client.

Summa Accountancy Services Limited understands that it must comply with the requirement to identify and verify all beneficial owners or person purporting to act on the client before establishing a business relationship or the carrying out of an occasional transaction.

R.30(3) goes on to explain that the Firm may as soon as practicable after first contact with a client, undertake its client verification steps during the course of the establishment of business relationship provided that the following apply:

- That the verification during the establishment of the business relationship is necessary not to interrupt the normal course of business
- There is little risk of ML/TF

Summa Accountancy Services Limited is committed to identifying and verifying clients as soon as possible and before undertaking any work on behalf of a client.

The Firm is further aware that under R.33 MLR 2017 that it must undertake it’s enhanced due diligence measures if it discovers that a client has provided false or stolen identification documentation or information.

The Firm is aware of its obligations under R.28(11) MLR 2017 to conduct on-going monitoring of business relationship to ensure:

- That the transactions undertaken through the course of the relationship with the client are consistent with the Firm's knowledge of the customer, the customer's business and risk profile
- Reviewing existing records and keeping documents or information obtained for CDD up-to-date

Requirement to Cease Transactions

Summa Accountancy Services Limited is aware of R.31 MLR 2017 and will not establish a business relationship, carry out a transaction or continue to act for an existing customer where Summa Accountancy Services Limited has been unable to apply its CDD measures.

New Products, New Business Practices (Including New Delivery Mechanisms) or New Technology

The firm is aware of the need to assess and mitigate any potential Money Laundering or Terrorist Financing risks associated with the adoption of any new products, new business practices (Including new delivery mechanisms) or new technology.

CDD/EDD Record Keeping

Summa Accountancy Services Limited keeps copies of documents and information used to perform its identification and verification.

This is recognised as helpful to evidence the steps that Summa Accountancy Services Limited has taken and also provide useful information to law enforcement should a client be subject to an investigation.

The Firm has a commitment to keep records necessary to demonstrate its compliance with AML/CTF commitments and obligations and these are explained later in the policy.

Impersonation Risk

Summa Accountancy Services Limited is mindful of the risk of a someone trying to impersonate someone else. Summa Accountancy Services Limited's policy on seeing original, certified or biometric verification of identification of individuals who are clients or beneficial owners of clients will help to confirm that the person that Summa Accountancy Services Limited is dealing with is the person that they claim to be.

Summa Accountancy Services Limited is mindful of the possibility that an individual may seek to use fake identity documents; this is a further reason that copies of documents provided as evidence are copied and stored.

Internal Controls

Summa Accountancy Services Limited is aware that it is important that it monitors the implementation of its AML/CTF policies and procedures to ensure that such policies and procedures are correctly followed or if any variation occurs is approved by senior management of Summa Accountancy Services Limited.

R.21 MLR 2017 reflects the reality that the AML/CTF compliance structure of a sole practitioner firm will vary to that of a multi-person firm.

R.21(6) refers to an individual who neither employs of nor acts in association with another person as needing a different control AML/CTF control structure.

MLR 2017 also introduces the impact of a Firm's AML/CTF systems and controls of the size and nature of the Firm. It should be implied that a sole practitioner Firm is not at risk of being exposed to ML/TF.

Summa Accountancy Services Limited is conscious it will need to consider its resources as to whether it is sufficiently resourced with senior management with the appropriate skills, knowledge and expertise to appoint deputies to the roles discussed below, in particular, the Nominated Officer (NO) and/or the Money Laundering Compliance Principal (MLCP).

There is a requirement for a Firm which is not a sole practitioner to inform its AML supervisor within 14 days of the appointment of both of the following:

- Who is the Nominated Officer (NO) for the Firm?
- Who is the person responsible for the Firm's compliance with MLR 2017 (The Money Laundering Compliance Principal (MLCP))?

There is a requirement for the Firm to have a NO and MLCP unless it is a sole practitioner as defined above.

The Nominated Officer of Summa Accountancy Services Limited is (automatically inserted, may need to show a deputy).

The Money Laundering Compliance Principal of Summa Accountancy Services Limited is (automatically inserted, may need to show a deputy).

The appointment of a NO (Nominated Officer) is a requirement under both MLR 2017 and POCA 2002 and is the person responsible for receiving Suspicious Activity Reports (SARs) from staff within the Firm and for determining from such internal SAR reports whether a SAR should be made to the National Crime Agency (NCA) and if required making SAR reports to the NCA.

The Money Laundering Compliance Principal is a requirement of MLR 2017 and is the person within the Firm who is responsible for Firm's compliance with MLR 2017. The MLCP should be an officer of the Firm (or equivalent if there is no board) or a member of the Firm's senior management.

It is clear then, that for a sole practitioner firm the individual who is the sole practitioner undertakes both the roles of the NO and the MLCP as there is no one else to undertake these roles. Being a sole practitioner does not mean that the roles of the NO and MLCP do not need to be undertaken only that the titles of the role are not required as it can only be the sole practitioner who undertakes this role.

The Firm must also consider whether it will benefit from the appointment of an individual to be responsible for the role of Independent Audit Function (IAF). Whether the Firm has chosen to introduce an Independent Audit Function will depend on its size and nature.

Though not specifically defined the size and nature of the firm is both, factual by the size of the firm by, for example employee number or turnover, and risk based, for example the geographical reach of the Firm and the scope of work undertaken by the firm. From this, the firm will have to have regard to the outcome of both its own Firm Risk Assessment and the Risk Assessment undertaken on its clients.

R.19 (5) MLR 2017 that a regulated firm should consider both guidance issued by the FCA or any supervisory authority or appropriate body approved by the HM Treasury when consider what is appropriate and

proportionate with regard to the size and nature of its business.

If established the Independent Audit Function's duty include:

(i) to examine and evaluate the adequacy and effectiveness of the policies, controls and procedures adopted by the relevant person to comply with the requirements of these Regulations;

(ii) to make recommendations in relation to those policies, controls and procedures; and

(iii) to monitor the relevant person's compliance with those recommendations.

Summa Accountancy Services Limited **has/has not** decided to set up an Independent Audit Function

The firm is aware that is would not be unusual that the same individual may be the both the NO and MLCP for the Firm. This combined role is also known as the Money Laundering Reporting Officer (MLRO) which is the title that many within the regulated sector may be familiar with.

Whilst it is not a requirement of MLR 2017 or POCA 2002 to have an MLRO it may be sensible to continue with this title for ease of reference of employees of the Firm.

Employee Screening

Summa Accountancy Services Limited carries out screening of relevant employees in accordance with r.21(1)(b) MLR 2017 both before the appointment is made and during the course of employment.

Summa Accountancy Services Limited is aware that where the firm is a strict sole practitioner as explained within the Internal Controls section of this policy that it will be unable to and not obliged to carry out Employee Screening steps.

Summa Accountancy Services Limited acknowledges that screening means r.21(2)(a) means an assessment of:

(i) the skills, knowledge and expertise of the individual to carry out their functions effectively;

(ii) the conduct and integrity of the individual;

Summa Accountancy Services Limited also acknowledges that relevant employees r.21(2)(b) are employees whose work is:

(i) relevant to the relevant person's compliance with any requirement in these Regulations, or

(ii) otherwise capable of contributing to the–

(aa) identification or mitigation of the risks of money laundering and terrorist financing to which the relevant person's business is subject, or

(bb) prevention or detection of money laundering and terrorist financing in relation to the relevant person's business.

Records

Summa Accountancy Services Limited recognises that the records that are kept in relation to all aspects of its AML/CTF compliance are very important. Summa Accountancy Services Limited recognises that such records will form evidence of its compliance to its AML supervisor and interested law enforcement agencies.

Summa Accountancy Services Limited recognises that its AML/CTF records will be its defence against any criticism or prosecution. Deficiencies in its records will prima facie indicate that such compliance work has not been undertaken by the firm.

Summa Accountancy Services Limited is aware that the MLR 2017 R.40 sets out the requirements for AML records that Summa Accountancy Services Limited must retain in relation to the following:

- Copy documents and information obtained to satisfy CDD requirements
- Sufficient supporting records of any transaction that is the subject of CDD or ongoing monitoring to enable the transaction to be reconstructed

Summa Accountancy Services Limited is aware of the requirements of R.40 MLR 2017 with regards to retaining the records required under (R.40 MLR 2017) as described above for a period of at least five years after the following events occur R.40(3) MLR 2017:

a) that the transaction is complete, for records relating to an occasional transaction; or

b) that the business relationship has come to an end for records relating to–

(i) any transaction which occurs as part of a business relationship, or

(ii) customer due diligence measures taken in connection with that relationship.

Summa Accountancy Services Limited will usually issue a client dis-engagement letter at the point that events laid out in R.40(3) above have occurred. The firm uses the issuing of the dis-engagement letter as the start of the five-year period.

Summa Accountancy Services Limited is aware of the requirements of R.40 MLR 2017 to delete any personal data of a client after a period of five years unless (R.40 (5)(a)):

(i) by or under any enactment, or

(ii) for the purposes of any court proceedings;

(b) the data subject has given consent to the retention of that data; or

(c) the relevant person has reasonable grounds for believing that records containing the personal data need to be retained for the purpose of legal proceedings.

Summa Accountancy Services Limited is aware that for a continuing client, it is not required to keep records listed in R.40(3)(b)(i) for more than ten years; which are records relating to:

(i) any transaction which occurs as part of a business relationship,

Summa Accountancy Services Limited is also aware of R.19 MLR 2017 which requires that Summa Accountancy Services Limited must maintain a record in writing of:

- The policies, controls and procedures
- Any changes as a result of updates or reviews
- The steps taken to communicate these and any changes within Summa Accountancy Services Limited's business

The AML/CTF records held may include

- AML/CTF Policy document
- AML/CTF Procedures document
- Sector Risk Assessment
- Firm Risk Assessment
- Evidence of compliance with the policies and procedures
- New Client Information forms
- Evidence of identification and verification work undertaken on clients' beneficial owners for CDD purposes
- Records to support any transactions subject to CDD or ongoing monitoring (sufficient to reconstruct the transaction)
- Client Risk Assessment forms
- Evidence of Risk Assessment updates
- Technical Reference Documents
- Training undertaken by any senior members of Summa Accountancy Services Limited
- Training undertaken by any staff of Summa Accountancy Services Limited
- Record of communication to staff of any review or changes to policies, controls and procedures

Where Summa Accountancy Services Limited structure requires:

- Senior management approval for any cash received by Summa Accountancy Services Limited
- Senior management approval of Summa Accountancy Services Limited accepting a PEP or their family members or close associates as a client

These documents are held in one or more of the following formats:

- AMLCC Online AML/CTF Compliance Tool
- Hard Copy Documents
- Electronic Documents

The firm is aware of the term "size and nature" of the Firm that is referred to within MLR 2017 with regards to the extent of policies, controls and procedures of any firm. Reference to some suggested records that might be considered to be kept by a larger or more risk exposed firm are listed within the draft sourcebook issued by OPBAS (Office of Professional Body Anti-Money Laundering Supervisors) is as follows:

- organisation chart;
- legal entity chart;
- job descriptions of senior management;
- composition of committees;
- documents setting out internal procedures and controls;
- internal audits of compliance with internal procedures and controls;
- external auditor's reports;
- compliance reports;
- data on suspicious activity reports and other engagement with law enforcement
- agencies;

- breach logs;
- review of information from other sources: information and alerts could come from
- law enforcement, other supervisors, employees, other businesses, or the public.

Data Protection

In accordance with R.41 MLR 2017, any personal data obtained by Summa Accountancy Services Limited for the purposes of its AML/CTF compliance will only be processed for preventing ML or TF.

Summa Accountancy Services Limited provides information to new clients relating to data protection before establishing a business relationship or undertaking an occasional transaction.

Summa Accountancy Services Limited will not, without due reason, retain personal data obtained for purposes of AML/CTF beyond a period of five years from the end of a business relationship or completion of an occasional transaction. Further details are covered in the Records section of this policy.

Reliance on Third Parties

It is not the intention of Summa Accountancy Services Limited to rely upon information held by Third-Parties to assist with its AML/CTF other than through information placed on the AMLCC online compliance platform.

Should Summa Accountancy Services Limited consider placing reliance on a third party to apply it Customer Due Diligence (CDD) measures then it is aware that it is the Firm that remains liable for any failure to apply it CDD measures.

Summa Accountancy Services Limited will review and amend it AML/CTF policy should it vary from its current policy on Reliance on Third Parties.

Training and Internal Communication

Summa Accountancy Services Limited recognises that it has the best chance of preventing and identifying ML/TF using an "all eyes" approach. This means training everyone within Summa Accountancy Services Limited to understand what activities or transactions might be identified as suspicious. This is to ensure that all staff understand the obligation to report suspicious activity or transactions to Summa Accountancy Services Limited's Nominated Officer (NO) for the purposes of reporting to the NCA under POCA 2002.

The firm is aware that the 2020 amendments to the regulations introduce a requirement to train all "agents" of the firm as if they were staff. Reference to training staff within this policy includes relevant agents. AMLGAS 8.2 provides clarity on who is an agent.

The firm is aware that where it contracts with third parties who provide accountancy services (as defined within MLR) to the firm that the third party should be either:-

- supervised for AML in their own right (for those accountancy services provided to the firm) or,
- a contract must exist between the firm and third-party that confirms the relationship meets all parts of the AML requirements.

Guidance on this point can be found on the Gov.uk website:

https://www.gov.uk/guidance/money-laundering-regulations-accountancy-service-provider-registration

The firm is aware that the 2020 amendments to the regulations introduce a requirement to train as “agents” of

the firm as if they were staff.

Summa Accountancy Services Limited further recognises its responsibility for ensuring that all staff are both aware of and understand how to apply Summa Accountancy Services Limited's own policies controls and procedures. Summa Accountancy Services Limited will communicate to staff any updates to any changes to its systems, policies, controls and procedures.

Summa Accountancy Services Limited is conscious that by training all staff then they are minimising the risk that ML/TF would go undetected by Summa Accountancy Services Limited. This approach to training support that view that all staff are relevant staff for R.21(2)(b) MLR 2017 and that such training forms part of the screening process required for both new and existing staff under R.21(1)(b).

If Summa Accountancy Services Limited using the services of individuals or entities to assist with the provision of its own client services then this will ensure that such non-employees are given or have received training on both AML/CTF its policies controls and procedures to the same standard Summa Accountancy Services Limited's employees.

A record of all AML/CTF related training is kept.

Further training is given after a maximum period of twelve months or as updates are required, whichever is sooner.

Reporting

Summa Accountancy Services Limited is aware that it has a role to play in preventing and identifying ML/TF. A key role in this is passing information to the NCA and where appropriate seeking authority from the NCA to continue with a transaction. Summa Accountancy Services Limited will use the Suspicious Activity Reporting facility to make reports to the NCA when activity or transactions required reporting to the NCA.

All reports to the NCA will be made by Summa Accountancy Services Limited's Nominated Officer (NO) or its Deputy NO if one has been appointed. The Suspicious Activity Reports (SAR reports) made or considered by the NO are likely to have come from internal SARs made by employees of the Firm to the NO.

Evidence is held with Summa Accountancy Services Limited's AMLCC online compliance tool that relevant members of Summa Accountancy Services Limited have been trained in both the law and guidance relevant to AML/TF that is relevant to the services provided by Summa Accountancy Services Limited and Summa Accountancy Services Limited own internal policies and procedures relevant to AML/CTF.

Why Report?

Summa Accountancy Services Limited is aware that its obligation to report to the National Crime Agency (NCA) is set out in Part 7 Proceeds of Crime Act 2002 (POCA) and Part 3 of the Terrorism Act 2000 TACT.

All employees of the firm are obliged to report to the Nominated Officer any activity that they consider may be money laundering or terrorist financing. Further details of what to report are within the **What to Report** section of this policy.

All employees of the firm are aware that their best defence under both POCA and TACT is to make a report to the Firm's NO.

Tipping Off: All employees of the firm are also aware that they MUST NOT disclose to any party that is the subject of a SAR (tipping off), that a SAR has been made or that an investigation by law enforcement is ongoing

(prejudicing an investigation).

What to Report?

Summa Accountancy Services Limited is aware of the details laid out in the Summa Accountancy Services Limited Approach to AML/CTF section of this policy, which lays out the principle money laundering offences that are reportable.

Any uncertainty on whether to report or not by employees of the firm should be discussed with NO of the firm.

Any uncertainty on behalf of the firm's NO should be discussed with the firm's senior management, the Firm's AML supervisor or independent legal advice sought.

It is often wise for the firm, if seeking independent advice on a SAR, not to disclose the client details as this will minimise the risk of a tipping off offence under POCA.

Cash Handling

Summa Accountancy Services Limited is aware of the difficulty of tracing the source and movement of cash.

Summa Accountancy Services Limited has considered the risk of handling the proceeds of crime by accepting cash from any client either in payment for fees already incurred or expected to be incurred in the future or for payment of any liabilities on behalf of the client. The Firm has taken a view that it will only accept any cash from a client provided the client can evidence with independent records or information the source of the cash.

Any such acceptance of cash by Summa Accountancy Services Limited will require senior management approval.

Client Account

Summa Accountancy Services Limited has a policy of operating a client account to hold any funds that belong to clients of the Firm.

The client account is used only for the receipt of refunds from HMRC on behalf of clients.

The firm is careful to be sure that any payments from the client account are only made to accounts of the named client and are not paid to any third-parties.

Summa Accountancy Services Limited is conscious that funds paid out if its client account will often be seen as "clean" funds and the firm is therefore aware of the risk the clients with criminal intent may seek to use the Firm's client account as a way of demonstrating "clean" funds to a third-party.

The client account will be reconciled on a monthly basis and discrepancies investigated and resolved. Such reconciliations will be checked by a senior member of the firm and evidence of such a check recorded.

Summa Accountancy Services Limited will be clear to have documented authority from a client before drawing funds from the client account to cover invoiced fees of the firm incurred for work on behalf of the client.

The firm is also aware that a client being prepared to deposit funds in advance of work being undertaken by the Firm and then seeking to recover the deposit by cancelling the instructions to the Firm is a route that could be used to "clean" funds through the firm's client account.

AML Supervision

Summa Accountancy Services Limited can confirm that it is registered with a relevant AML supervisor.

Summa Accountancy Services Limited is supervised for AML by International Association of Bookkeepers

Summa Accountancy Services Limited is also aware that if it undertakes work that is classified as TCSP work that it will need to be registered on any TCSP register held by HMRC. Such a register of TCSP service providers is a requirement placed on HMRC by MLR 2017. Being listed on such a register is not a substitute for the firm being supervised for AML for any services that it provides that are regulated services under MLR 2017. At the time of drafting this policy the firm is aware that no such register is in place at HMRC and that it will need to monitor for updates. It is likely that the Firm's AML supervisor for TCSP work will provide the firm's information to HMRC for registration on the TCSP list, the Firm will monitor this.

Summa Accountancy Services Limited is aware of the requirement that on or before 26th June 2018 that it will need to have authority from its AML supervisor to continue to operate Summa Accountancy Services Limited. Such authority will be subject to Summa Accountancy Services Limited confirming that none of its beneficial owners, officers or senior managers have an unspent conviction which is a relevant conviction on Schedule 3 of MLR 2017.

Summa Accountancy Services Limited does not have any of its beneficial owners, officers or senior managers that have a current conviction which is a relevant conviction for Schedule 3 MLR 2017.

Summa Accountancy Services Limited is also aware of its obligations to appoint (where appropriate) and to inform its AML supervisor of the appointment of any person responsible for the compliance of Summa Accountancy Services Limited with MLR 2017 and the Nominated officer and any subsequent changes to these positions.

Prohibitions and Approvals - (firm must be authorised in relation to relevant criminal convictions)

Summa Accountancy Services Limited is aware of the requirement not to have anyone who has been convicted of a relevant criminal conviction (listed in Schedule 3 MLR 2017) as Beneficial Owner of Summa Accountancy Services Limited or as an officer or manager of Summa Accountancy Services Limited.

Confirmation of this will be provided to Summa Accountancy Services Limited's AML supervisor(s) once the format for such authorisation applications have been set out by Summa Accountancy Services Limited's supervisor(s). Authorisation will be requested prior to 26 June 2018.

Summa Accountancy Services Limited will update its authorising body within 30 days of any relevant convictions being made to the relevant parties of Summa Accountancy Services Limited.

Financial Sanctions and Proscribed Terrorist Groups or Organisations

Summa Accountancy Services Limited is aware of guidance issued by the Office of Financial Sanctions Implementation (OFSI) which is available online at: https://www.gov.uk/government/publications/financial-sanctions-faqs and the OFSI guidance on the associated monetary penalties at: https://www.gov.uk/government/.../Monetary_penalties_for_breaches_of_financial_sanctions.pdf

Summa Accountancy Services Limited is aware of the consolidated list of financial sanctions target issued by OFSI and is conscious that this is regularly updated.

The firm is aware that at 11pm on 31 December 2020 the Sanctions and Anti-Money Laundering Act 2018 (Sanctions Act) came into force. The Sanctions Act replaces former EU sanctions related law with autonomous UK sanctions law.

As a UK Accountancy Service Provider (ASP) the firm is obliged to comply with the Sanctions Act. The Office of Financial Sanctions Implementation (OFSI), "The Office of Financial Sanctions Implementation (OFSI) helps to ensure that financial sanctions are properly understood, implemented and enforced in the United Kingdom." Is a key resource in the area of UK financial sanctions.

You can view or search the "consolidated list" of sanctions targets on the OFSI website. It is recommended that you sign up to the free OFSI email alerts. You must report breaches of financial sanctions to OFSI. A form to use to report a breach is available on the OFSI website and must be emailed to OFSI. Failure to comply your obligations under the Sanctions Act could lead to criminal prosecution or a monetary fine.

If financial sanctions are unfamiliar to you, recommend reading the guidance on the OFSI website. Please be aware that if your firm operates in jurisdictions outside of the UK, different sanctions list and restrictions are likely to apply.

The firm should also be aware of the Proscribed Terrorist Organisations list. This is a list of terrorist organisations banned under UK law.

An extract from the OFSI Financial Sanctions Guidance is included below:

3.1.2 What must you do?

If you know or have 'reasonable cause to suspect' that you are in possession or control of, or are otherwise dealing with, the funds or economic resources of a designated person you must:

1 freeze them

2 not deal with them or make them available to, or for the benefit of, the designated person, unless:

2.6 there is an exception in the legislation that you can rely on; or

2.7 you have a licence from OFSI

3 report them to OFSI (see Chapter 5 of this guide).

MoRiLE Category
Reasonable cause to suspect refers to an objective test that asks whether there were factual circumstances from which an honest and reasonable person should have inferred knowledge or formed the suspicion.

A breach of these requirements may result in a criminal prosecution or a monetary penalty.

The Firm will be reviewing the OFSI consolidated periodically to be sure that clients of the Firm do not appear on this list. Should a client show on the list the Firm is aware of its obligation to notify OFSI immediately. A link to the OFSI consolidated list is here: https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets

Summa Accountancy Services Limited is aware of the Proscribed Terrorist Groups or Organisations list of banned organisations under UK law. A link to the list is here: https://www.gov.uk/government/publications/proscribed-terror-groups-or-organisations--2

The firm is conscious of the sense in reviewing this list periodically to be sure that clients of the Firm do not appear on this list.