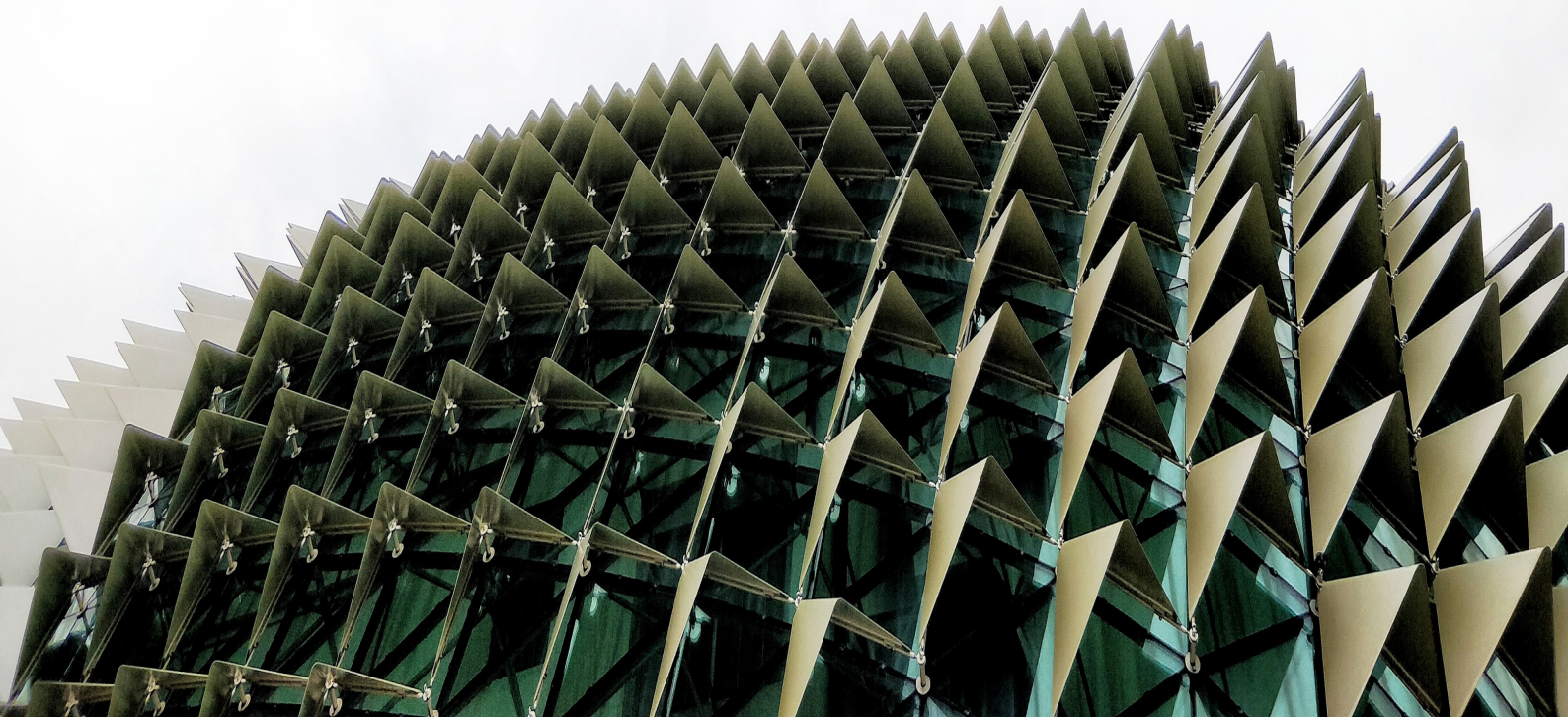
Improving AML/KYC/CTF Due Diligence Processes: Centralisation and the Benefits of a Digital Solution

OCTOBER 2020



Executive Summary

Money laundering and the financing of terrorism have a detrimental effect on the reputation of individuals, businesses, governments and for society as a whole. To tackle these threats, financial entities are required to perform anti-money laundering ('AML'), counter-terrorism financing ('CTF') and know your customer ('KYC') checks which are designed to identify potential bad actors. Robust customer due diligence ('CDD') is one element of an overall risk management architecture that can mitigate these threats.

While CDD measures have proven to be highly successful in tackling economic crime and greater emphasis has been put on global harmonisation, there are still large inefficiencies which are placing a significant cost and administrative burden on financial services firms and investors. The challenges faced by investment managers, fund administrators, fund governing bodies as well as regulators prevent, in many instances, an efficient CDD process from being developed and utilised within and across jurisdictions. This paper suggests a range of options that could be implemented that would improve the CDD process and would create scenarios in which compliance with AML, CTF and KYC requirements are safeguarded, while strengthening the role of regulators as standard setters.

The options explored in this paper can operate in conjunction with each other or provide a building block for other, more transformative, solutions to be implemented.

Option 1: Allow a regulated entity performing its own due diligence to pool due diligence efforts within its own organisation:

This option would allow a regulated entity performing CDD with respect to multiple funds (and other investors where relevant) to only have to perform CDD once for each individual/entity as a single process. This would result in the investor being subjected to substantially fewer documentation requests and the regulated entity's CDD process would be streamlined. In addition, regulators would have a better understanding of the investor than it would if multiple disparate files had to be accessed.

Option 2: Allow a regulated entity performing due diligence for others on an outsourced or delegated basis to pool due diligence efforts:

Fund administrators which perform due diligence for funds and investment managers on an outsourced/delegated basis are typically required to perform CDD separately for each fund, regardless of any overlapping investors. If the fund administrator were able to apply pooled effort, it would reduce the documentation requests investors are subjected to while streamlining the fund administrator's CDD process, resulting in significant cost savings.

Option 3: Allow a regulated entity to perform due diligence for others on a reliance basis with regard to the requirements of a single country:

A further improvement on options 1 and 2, and best operated in conjunction with those options, would be to establish a new regulated activity category for entities (i.e., a third-party provider) to perform CDD centrally and on a reliance basis for other regulated entities. These centralised due diligence processors ('CDDPs') would perform all of the CDD requirements for regulated entities while the underlying obligations on regulated entities would remain as a backstop. As the regulator will be directly supervising the CDDP, there can be closer supervision of the direct workings of the CDD and less variation in approach taken and judgment calls applied as fewer entities will be involved.

Option 4: Allow a regulated entity to perform due diligence for others on a reliance basis with regard to the requirements of multiple countries:

A logical extension of option 3 would be for the CDDP to seek authorisation from multiple countries to perform centralised CDD for regulated entities. These multi-country centralised due diligence processors ('MCDDPs') build on the digital ID ecosystem, as introduced by the Financial Action Task Force (FATF), by creating a standardised digital identity framework allowing MCDDPs to work within and across jurisdictions. Regulatory access would not be restricted, while efficiency would be further increased for investors and regulated entities using this facility.

Options 3a/4a: Use a digital solution to amplify Option 3 or Option 4:

This option would create a portable digital identity framework and allows the MCDDP, in addition to performing CDD on behalf of regulated entities, to use the unique ID code issued to the investor to be used at other regulated entities and would eliminate the need for a multitude of individual CDD checks having to be performed.

* * *

While we are mindful of the range of practical challenges that will need to be overcome if any of these options are to be implemented, they provide useful tools to streamline CDD practices, promote closer cooperation between the public and private sector and encourage a harmonised and interoperable ecosystem. In particular, the use of a portable digital identity could have the potential to improve and transform global CDD practices while providing all parties involved a high degree of comfort and assurance that national and international standards are being met.

ABOUT AIMA

The Alternative Investment Management Association (AIMA) is the global representative of the alternative investment industry, with around 1,900 corporate members in over 60 countries. AIMA's fund manager members collectively manage more than $2 trillion in hedge fund and private credit assets.

AIMA draws upon the expertise and diversity of its membership to provide leadership in industry initiatives such as advocacy, policy and regulatory engagement, educational programmes and sound practice guides.

AIMA works to raise media and public awareness of the value of the industry.

AIMA set up the Alternative Credit Council (ACC) to help firms focused in the private credit and direct lending space. The ACC currently represents over 170 members that manage $400 billion of private credit assets globally.

AIMA is committed to developing skills and education standards and is a co-founder of the Chartered Alternative Investment Analyst designation (CAIA) – the first and only specialised educational standard for alternative investment specialists. AIMA is governed by its Council (Board of Directors).

TABLE OF CONTENTS

Remmert Keijzer
Associate Director, Asset Management Regulation, AIMA
rkeijzer@aima.org

Introduction

Investment managers use third parties — such as banks, broker-dealers, wealth managers and transfer agents — for a suite of services and transactions to facilitate a fund's investment activities. These services may include custody, valuation of assets, marketing, securities lending support, regulatory advisory, legal documentation, fundraising, and/or anti-money laundering ('AML'), know your customer ('KYC') and counter-terrorism financing ('CTF') checks, all of which raise operations and compliance challenges for the investment manager and the fund. In this paper, we have chosen to focus on the customer due diligence ('CDD') obligations associated with AML, KYC and CTF regulations.

Compliance with the CDD requirements of applicable AML/KYC/CTF regulations is a data heavy exercise as the subscription process for funds requires investors to provide a high volume of information to fund administrators. It requires, among other things, checking every single investor against a number of sanction lists, verifying whether they are Politically Exposed Persons ('PEPs'), performing counterparty checks and checking for adverse publicity in the press. The information required can in some instances vary depending on the jurisdiction in which the fund, the investment manager[1] and the fund administrator are each domiciled. Moreover, the manner through which this information is collected and how the specific questions are asked differ between jurisdictions. The exercise is made more challenging with heavy system requirements and multiple data sources.

The subscription process requires investors to provide certain information to a third-party administrator appointed by the fund to perform CDD on behalf of the fund and there is an expectation that the fund's investment manager will perform ongoing due diligence of that administrator on behalf of the fund directors to aid in their oversight of the delegation of these functions to the administrator. Much of the information required varies depending on the jurisdiction. Moreover, the way this information is collected and how the specific questions are asked differs from fund to fund even within the same jurisdiction.

In this paper we build on the recommendations made by the FATF in its *Guidance on Digital Identity*[2] (the 'FATF Guidance') which introduced the concept of digital identity service providers ('IDSPs') by exploring the concept of national and regional AML/KYC/CTF (multi-country) centralised due diligence processors ('M/CDDPs'). These entities would perform AML/KYC/CTF checks on a prospective investor on behalf of the investment manager. After successful completion of these checks, the investor would be issued with a portable digital ID which could then be used by the investor to invest in other funds or open other financial services accounts in a secure and speedy manner without having to go through additional detailed AML/KYC/CTF checks.

This solution would address the lack of standardisation and the ongoing regulatory updates that are placing a significant cost and administrative burden on financial services firms and investors.[3] In addition, this would also accelerate and enhance risk assessments of investors, investments, transactions, third parties and counterparties.

Although we believe the concept of MCDDPs is the most ambitious option presented, we also present in this paper other solutions that are potentially less costly in terms of resources or regulatory changes.

1 We have used the term investment manager in this paper for ease of reference. The investment manager for purposes of this paper, is the entity that is generally responsible for the day-to-day portfolio and risk management of a fund. The investment manager for purposes of this paper may be: (i) a discretionary investment manager; (ii) a non-discretionary investment advisor; (iii) a registered investment adviser under the U.S. Investment Advisers Act of 1940, as amended; (iv) an alternative investment fund manager as defined in Article 4(1)(b) of the Alternative Investment Fund Managers Directive (2011/61/EU); or (v) a UCITS management company as defined in Article (2)(1)(b) of the UCITS Directive (2009/65/EC).

2 See https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf.

3 For example, according to the GLEIF (2018), sales people in banking spend 27% of their working week onboarding new client organisations (see https://www.gleif.org/en/newsroom/blog/gleif-identifies-that-over-half-of-salespeople-in-banking-spend-27-of-their-working-week-onboarding-new-client-organizations.

Current challenges from CDD

In financial services, the CDD process is challenged by the problem of the many:

- Many countries have adopted a regulatory regime designed to prevent and detect money laundering and counter terrorism financing, each of which varies from the others to a greater or lesser extent;[4]
- Many financial services firms are directly required by regulation to perform CDD with respect to the owners/beneficial owners of each account, often multiple times during the life of an account;[5]
- Many financial services firms outsource their CDD processes to other financial services firms, which may or may not be regulated by the same regulator resulting in the requirements for multiple countries having to be applied to an investor as part of a single process by these outsourced service providers;
- Many regulators are charged with supervising the CDD performed by regulated firms (or outsourced by them to other firms which may be inside or outside the jurisdiction and which may or may not be supervised by that regulator) in compliance with the local regulatory regime, which they do with varying levels of intensity;
- Many countries have different, and sometimes diverging or conflicting, interpretations of applicable regulations and differing approaches in designing and executing national CDD compliance;[6]
- Many individuals and entities will have more than one financial services account, and the vast majority of adults will have at least a bank account; and
- Many documents must be produced and many records must be kept for each instance of CDD performed.[7]

This translates into millions of documents and records and an extraordinary amount of full-time equivalent hours of time for processing, recordkeeping and regulatory supervision.

Figure 1 is a simplified visual representation of how CDD often proceeds currently in the alternative asset funds space.

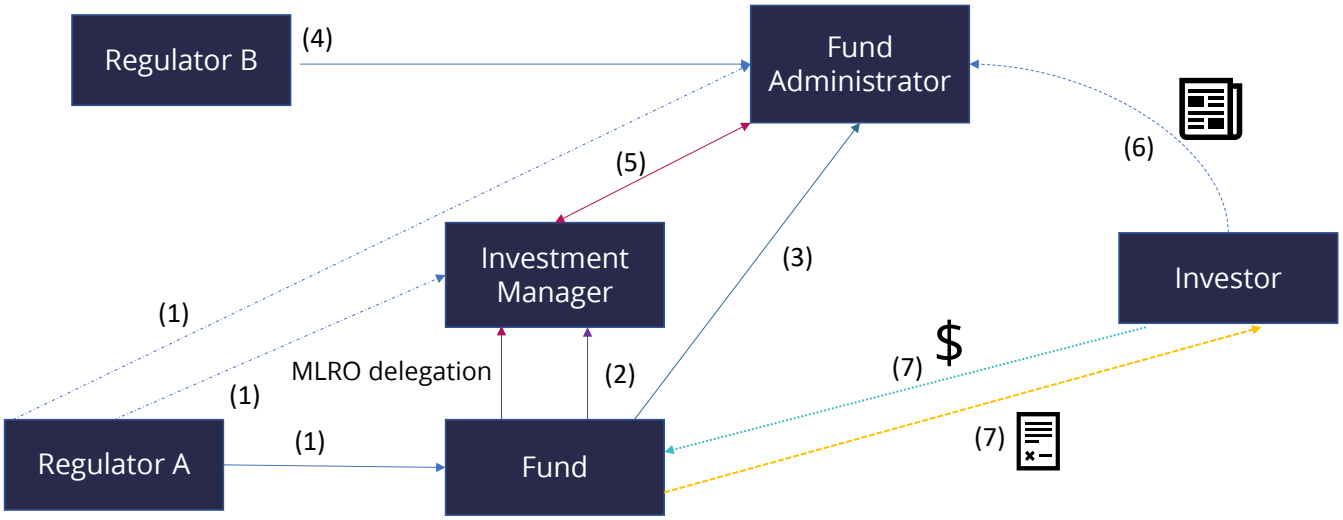
4 For example, the European Union ('EU'), through its anti-money laundering directives, applies a 25% threshold of ultimate beneficial ownership ('UBO') identification but in other jurisdictions, for example the Caymans Island and Guernsey, this threshold is 10%.

5 Article 14(5) of the EU's Fifth Anti-Money Laundering Directive ('AMLD5') requires that obliged entities must refresh due diligence for an existing customer on a risk-sensitive basis, or when the relevant circumstances of a customer change, or when the obliged entity is under any legal duty to contact a customer in the course of a calendar year for the purpose of reviewing any information which (i) is relevant to the risk assessment of that customer; and (ii) relates to the beneficial ownership of the customer.

6 For example, if the fund is a real estate fund registered in the United Kingdom, it will have to not only comply with AML/KYC/CTF regulation as issued by the Financial Conduct Authority, but also with guidance issued by the Royal Institute of Chartered Surveyors, the global professional body overseeing surveyors. In addition, the Joint Money Laundering Steering Group, a private sector body that is made up of leading UK trade associations in the financial services industry, has also issued sector specific guidance on CDD. In the Republic of Ireland, there are different levels of drill down with regards to UBO requirements depending on the interpretation of CDD rules by fund administrators, thereby creating challenges for funds, investment managers, investors and third parties.

7 For individuals, it is not uncommon to provide up to 16 different forms of documentation, which includes, but are not limited to, proof of address and source of funds and wealth, passport or national ID card, tax self-declaration form, professional investor form, and screening documents. When the above-mentioned documents need to be updated, the investor will need to submit all these documents again. Additionally, certain other correspondence may also be required to be filed, adding to the documentation burden. If the individual is deemed to be high-risk by an entity performing CDD, the documentation will need to be resubmitted or updated on an annual basis. For simple and standard corporate investor clients, the quantity of required documentation to be submitted is even higher as the passports or national ID card, proof of address and specimen signature sheets of all the shareholders (above a certain threshold) and the directors will need to be submitted, in addition to all the corporate documentation required, such as a certificate of incorporation, articles of association, register of directors and members, account opening forms and board resolution regarding signatories, audited financial statements, trading records, etc. It is not uncommon for simple and standard corporate client investors to submit in excess of 25 documents. However, for more sophisticated corporate investors the number of documents to be submitted is far higher.

Figure 1



Notes:

(1) Where the fund is established may determine which regulatory rules must be followed by the fund and its service providers (and delegates) with respect to CDD.

(2) At the start of the life of a fund, the fund's governing body appoints an investment manager. The appointment is memorialised by an investment management agreement that details the services to be provided, which typically includes provisions for the investment manager to assist in the supervision and oversight of the fund's other service providers, including the fund administrator. Although fund directors are tasked with providing oversight of the fund's service providers, they often delegate this to another party, such as the investment manager.

(3) At the start of the life of a fund, the fund governing body also appoints a third-party fund administrator. This relationship is governed by an administration agreement setting out the services to be provided, which typically include performing the CDD on fund investors and other AML, KYC and CTF related duties.

(4) In the alternative assets fund world, the fund administrator is often established in a jurisdiction other than the one where the fund was established.[8] However, it is typically the CDD requirements of the fund jurisdiction that determine the CDD performed by the fund administrator for the fund's investors.[9]

(5) With respect to CDD matters applicable to the fund due to the regulation applied by the competent authority of the fund's jurisdiction of establishment (Regulator A in the picture), other third-party service providers, such as the fund's third-party administrator, may or may not agree to perform the functions required of a fund's money laundering reporting officer ('MLRO'). In such instances, there may be an agreement pursuant to which an individual at the investment manager, or another third-party service provider, is appointed to be the fund's MLRO.[10] In which case there would also be an arrangement in place via which the fund's administrator (and the investment manager where a third-party service provider is engaged as the MLRO) would provide the information to the appointed MLRO necessary to perform that function.

(6) When a prospective investor wants to purchase shares/units of a fund, the prospective investor completes a subscription agreement, which includes questions designed to elicit the information needed to form the start of the CDD process. The prospective investor submits all relevant subscription and CDD paperwork to the fund administrator, which then proceeds to perform the

8 This is often because some jurisdictions have developed an expertise in, for example, fund servicing while others have developed an expertise in portfolio management.

9 A notable exception is Luxembourg where fund administrators are required to apply Luxembourg CDD standards, regardless of the jurisdiction of where the fund is domiciled.

10 We note, however, that in some jurisdictions, most notably in the United Kingdom, the fund is not allowed to delegate the role of MLRO to the investment manager.

CDD required by each of the applicable competent authorities (Regulator A and Regulator B in this case).[11]

(7) The fund, however, may only accept the prospective investor's subscription money (represented by the $ symbol in the picture) once the appropriate CDD has been completed. Once the CDD has been completed satisfactorily, the fund issues the relevant number of shares or units in the fund (represented by the document symbol at (7)) to the investor.

Current challenges experienced by investors, investment managers and fund governing bodies

Investors often identify the problems with the CDD system along the following lines:

1. Each investor has many accounts and often invests in many funds;
2. A potentially significant amount of identifying information – dependent on the investor's risk-rating - must be provided to open each account or make each fund investment;
3. For each account and fund investment, there is a frequent need to provide updated information and not all such requests are on synchronised timing;[12]
4. Investment managers can build up extensive knowledge of an investor but if the risk assessment undertaken by the fund administrator determines that simplified CDD is sufficient, the investment manager cannot relay this knowledge to the fund administrator as no further drill down is required under a prescribed risk-based approach;
5. Cross-border disclosure limitations with respect to investor information may exist between jurisdictions which may hamper the exchange of relevant CDD information; and
6. Investors are often represented by investment advisors during the CDD process which can lead to a more protracted communication process between the investor and the fund, the investment manager and/or fund administrator during the CDD life cycle.

CDD regulations make no provisions for administrative efficiency in the investment funds context.[13] For example, there is:

- No sharing in most cases of CDD processes for multiple funds with the same investment manager;[14]
- No sharing of due diligence processes for multiple funds with the same fund administrator unless this has been agreed in the terms set out in the subscription agreement and there are no General Data Protection Regulation (EU) 2016/679 ('GDPR') or other data protection restrictions applicable; and
- Often no reliance permitted when other intermediaries in the chain have performed full CDD (e.g., a broker-dealer recommending a fund investment for one of its clients will have undertaken its own CDD prior to establishing the client relationship), and where reliance is permitted the attendant additional requirements can be operationally onerous. Investment managers and fund governing bodies often make similar observations.

11 See footnote 8.

12 The frequency with which ongoing CDD has to be performed is dependent on the risk-rating associated with the investor. Funds, investment managers and administrators operate a risk-based approach to determine the risk level associated with an investor. There is no necessity to re-verify investors – independent of whether these concern individuals or corporate investors – unless there are question marks as to the reliability, authenticity and accuracy of the data provided by them or if precipitated by a trigger event. For those investors defined as high-risk, a review of their accounts and documentation will usually occur every year. For investors whose risk-rating is medium, a review will occur every other year. Finally, investors defined as low-risk will be reviewed every three years. If the CDD reveals that additional due diligence is needed to resolve any anomalies, enhanced due diligence will be required to be undertaken which lengthens the process substantially.

13 As further explored in more detail below, regulated entities may, in some jurisdictions and instances, rely on third parties to conduct customer identification/verification at the onboarding stage. The fund, however, remains ultimately liable for any failure to comply notwithstanding its reliance on a third party.

14 This can, however, depend on the terms agreed in the subscription agreement around the sharing of data. However, if an investment manager manages funds that use different administrators, there can be no sharing of data.

Current challenges experienced by fund administrators

Fund administrators face slightly different challenges, such as:

1. Fund administrators appointed by an investment manager may have to apply the AML regulations applicable to the investment manager when performing CDD on fund investors;
2. Fund administrators appointed by a fund generally have to apply the CDD regulations applicable to the fund when performing CDD on fund investors;
3. Fund administrators are sometimes regulated financial services firms and subject to AML/KYC/CTF regulations imposed by their local regulator which requires them to apply the local CDD requirements to investors in funds they administer, regardless of the applicability of other requirements imposed as a result of having accepted the appointment by the investment manager and/or the fund itself;
4. The fund administrator, the investment manager and the fund are frequently in three separate jurisdictions;
5. Even if the three jurisdictions are all in the EU, the differences in transposition, interpretation and enforcement across the EU effectively make these jurisdictions all different for practical purposes;
6. For each account and fund investment, there is a frequent need to provide updated information and not all such requests are on synchronised timing;
7. CDD regulations make no provisions for administrative efficiency in the investment funds context. For example, there is:
    - No sharing in most cases permitted of CDD processes for multiple funds with the same investment manager;
    - No sharing in most cases permitted of CDD processes for multiple funds with the same fund administrator unless this has been agreed in the terms set out in the subscription agreement and there are no GDPR or other data protection restrictions applicable; and
    - Often no sharing permitted of personal data/information of investors among investment managers and fund administrators unless this has been agreed in the terms set out in the subscription agreement and there are no GDPR or other data protection restrictions applicable.

Current challenges experienced by regulators

For European regulators, the current CDD system presents some additional considerations:[15]

1. Differences in transposition, interpretation and enforcement of CDD regulations across the EU, effectively making these jurisdictions all different for practical purposes;[16]
2. Multiple (local) regulators, or different departments within the same regulator, request the same information from the same investment manager and fund administrator at different times and in different formats;
3. Findings of CDD non-compliance failures are often not shared between competent authorities, preventing other regulators from performing subsequent CDD checks; and

15 See European Banking Authority report on the future AML/CFT framework in the EU, available as of 10 September 2020 at https://eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2020/931093/EBA%20Report%20on%20the%20future%20of%20AML%20CFT%20framework%20in%20the%20EU.pdf.

16 Significant differentiation could be observed across Member States regarding the implementation of the AMLD4. For example, Ireland and Romania were referred to the European Court of Justice by the European Commission for not implementing AML rules and were ordered to pay a lump sum of EUR 3 million and EUR 2 million respectively (see: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200092en.pdf). In 2020, the European Commission referred Austria, Belgium and the Netherlands to the European Court of Justice for failing to fully transpose AMLD4 (see https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1228).

4. Most regulators rely on regulated entities' own assessments of the adequacy of their CDD systems and controls which, in effect, may not meet the required minimum standards as set by these regulators.

AIMA's suggestions

There are multiple possible ways to improve the process for the benefit of investors, regulated entities and regulators. We lay out a few of these below in ascending order of ambition, transformative change needed and perceived benefit to all involved. We note that some of these options can operate in conjunction with each other or provide a building block for other, more transformative, solutions to be implemented, as outlined below.

The options described below, if implemented, have the potential to transform current and widely used CDD practices, thereby making it quicker and less costly while providing all parties involved with a high degree of comfort and assurance. If the options are adopted as suggested, they have the potential to streamline current CDD practices and would elevate the standards and expectations regulators have as they would bring greater efficiency, all while reducing duplication and safeguarding the high standards set by regulators.

For these options to be adopted on a global level, we believe that a selection of financial jurisdictions who have either deep (financial) historical ties or who are willing to rely on each other's regulatory and supervisory framework could initiate these options and make possible operational and practical changes to the framework. For instance, the United Kingdom and Switzerland recently signed a joint statement regarding future mutual recognition and co-operation in financial services and which is intended to result in the recognition of each other's regulatory and supervisory regimes in, among others, the area of asset management.[17] Other jurisdictions which may be involved in the initial stages of exploring these options are the United States, Hong Kong, Singapore and the Cayman Islands. Following this, and dependent on the success of the various individual options, other jurisdictions may choose to adopt these too, thereby creating a global and uniformly recognised CDD framework.

An overview of the options, as well as their core assumptions, benefits and challenges can be found in Appendix A. All the options explored below are based on a high-risk investor with an annual CDD cycle.

Option 1: Allow a regulated entity performing its own due diligence to pool due diligence efforts within its own organisation[18]

Under current requirements, each regulated entity acting on behalf of funds is required to perform CDD separately for each fund regardless of any overlapping investors. On occasion, the regulated entity may be able to re-use earlier performed CDD findings, although this will be subject to updating. Regardless, an investor with investments in two funds managed by the same investment manager will be subject to two sets of due diligence requests with potentially differing timeframes. Figure 2 below illustrates this.

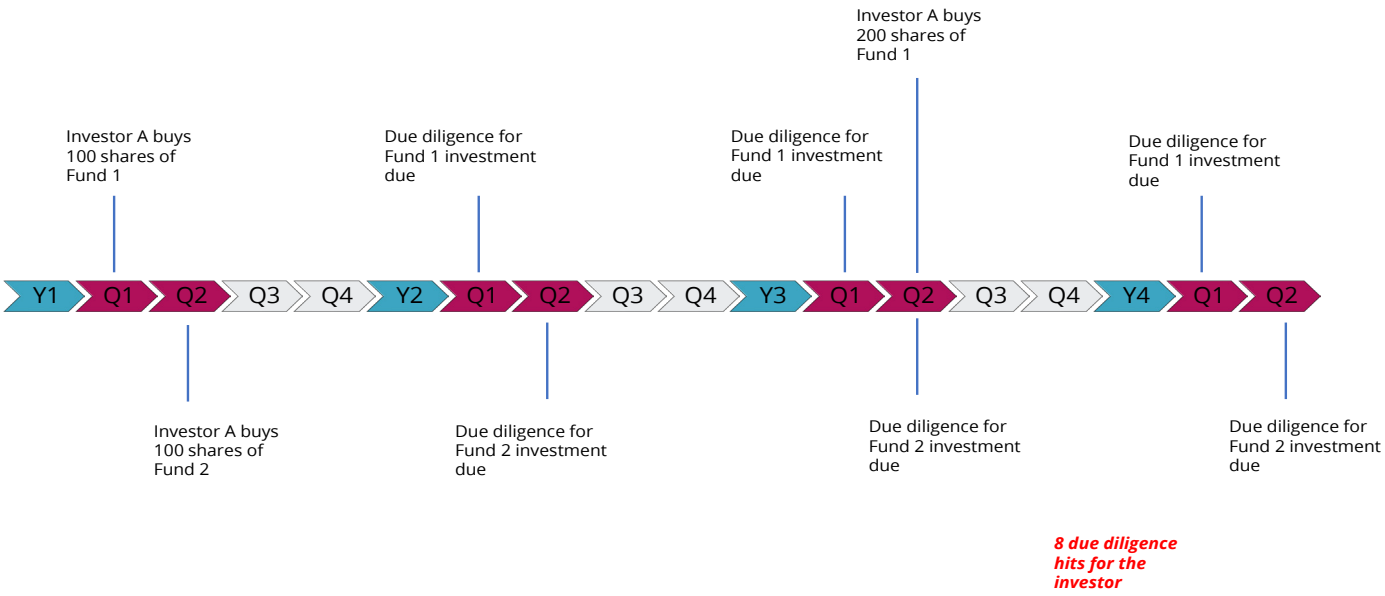
A simple and effective first step toward efficiency would be to allow a regulated entity performing CDD with respect to multiple funds (and other investors where relevant) to only have to perform CDD once for each individual/entity as a single process. In other words, when Investor A first invests (Fund 1), CDD is done. If Investor A then invests in another fund serviced by the same regulated entity (Fund 2) before the CDD on Investor A with respect to Fund 1 was due to be updated,[19] no new CDD would be required at that time.

17 See, e.g., https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/896778/Joint_Statement_between_Her_Majesty_s_Treasury_and_the_Federal_Department_of_Finance_on_negotiating_a_Mutual_Recognition_Agreement_on_financial_services.pdf.

18 We note that this option is already being utilised in practice by some fund administrators who have incorporated it through subscription agreements and the use of GDPR privacy notifications.

19 For ease of presentation, we have assumed that all of the investors shown in Figures 2-8 have been deemed high-risk and are therefore subject to annual CDD requirements. Although in the regular course most investors will be subject to less frequent CDD renewal requirements, there would also be many more of them.

Figure 2



When the Fund 1 CDD is then required to be refreshed, the refreshed collection for Investor A would count for both Fund 1 and Fund 2, syncing up the CDD cycle with respect to Investor A. This is illustrated in Figure 3.

Another variation of this theme could focus the re-synchronisation on events where the investor is otherwise engaging with the regulated entity for other reasons, i.e., a trigger event such as making an additional investment and therefore submitting additional subscription paperwork. This may result in more frequent updates from the investor overall but there would be fewer where the investor has not initiated the contact. This is illustrated in Figure 4.

Either of these variations would provide the following benefits, without any fundamental loss of CDD protection:

1. The investor would be subject to substantially fewer documentation requests;
2. The regulated entity's CDD process could be streamlined; and
3. If CDD were consolidated on an investor by investor basis rather than on a fund by fund basis, regulators would have a better picture of the investor than it would if multiple disparate files had to be accessed.

A challenge to overcome with this option is the need to be able to identify records attributable to each individual fund and possible restrictions of the sharing of these records under GDPR or other data protection regulations in other jurisdictions. On the latter, fund administrators with numerous offices globally may not be privy to the investments held within other offices and the possible leverage of documentation. Due to data protection regulations, the fund administrator may not currently be able to share or store across locations. Investors could, however, be asked to (voluntarily) sign data-sharing contracts at the onboarding stage but this could raise operational difficulties if, for example, only a small selection of the investors agree to this and the others do not.

We note that, in the instance an investor uses different special purpose entities to invest in two or more separate funds managed by the same manager, the obligation to perform separate CDD on these special purpose entities remains and cannot be amalgamated.

Figure 3

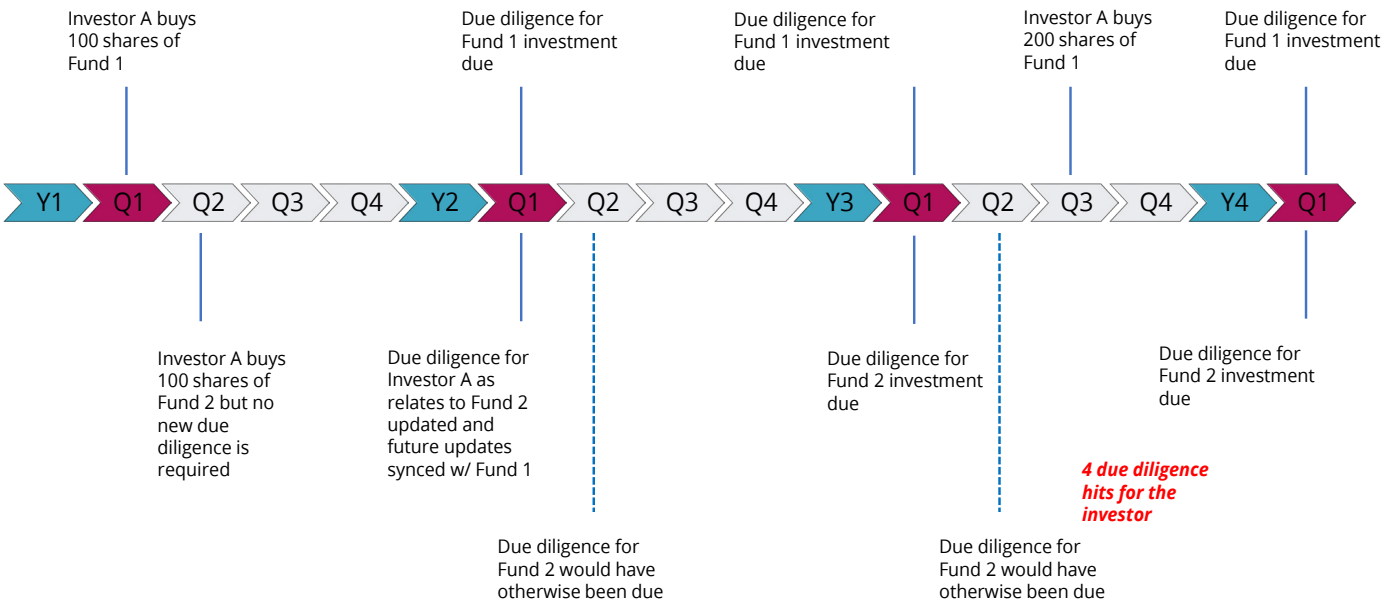
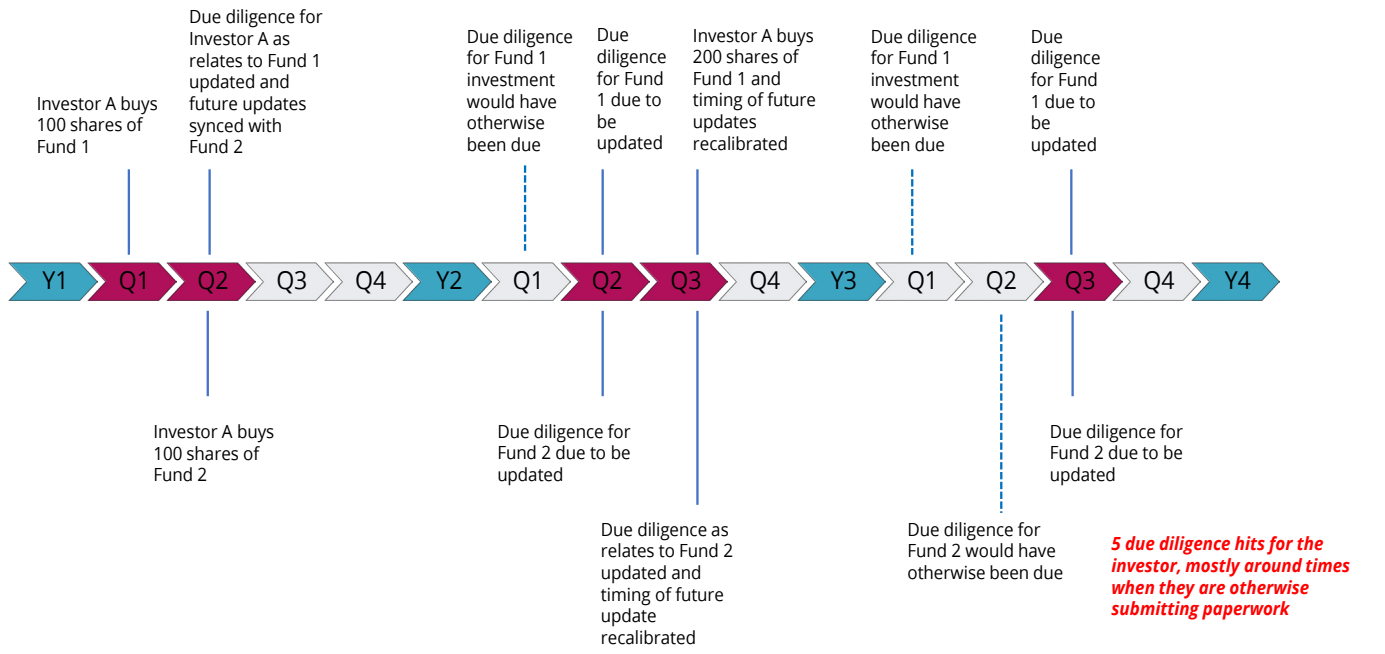


Figure 4

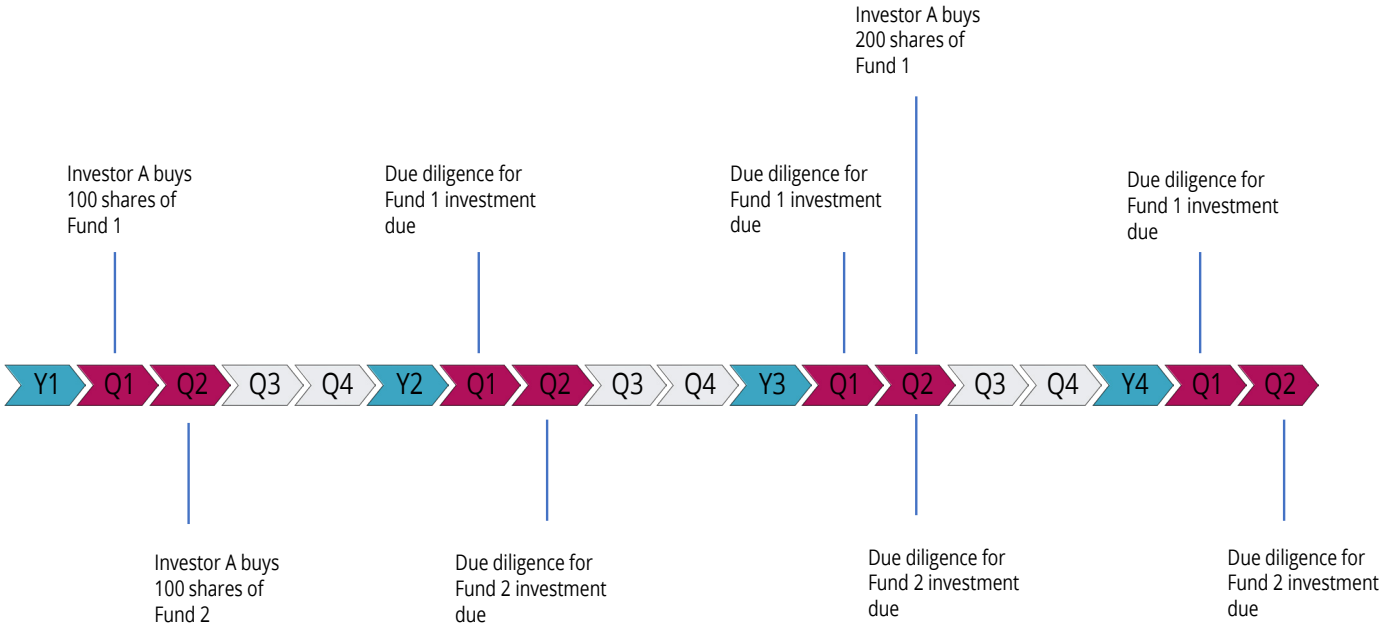


Option 2: Allow a regulated entity performing due diligence for others on an outsourced or delegated basis to pool due diligence efforts[20]

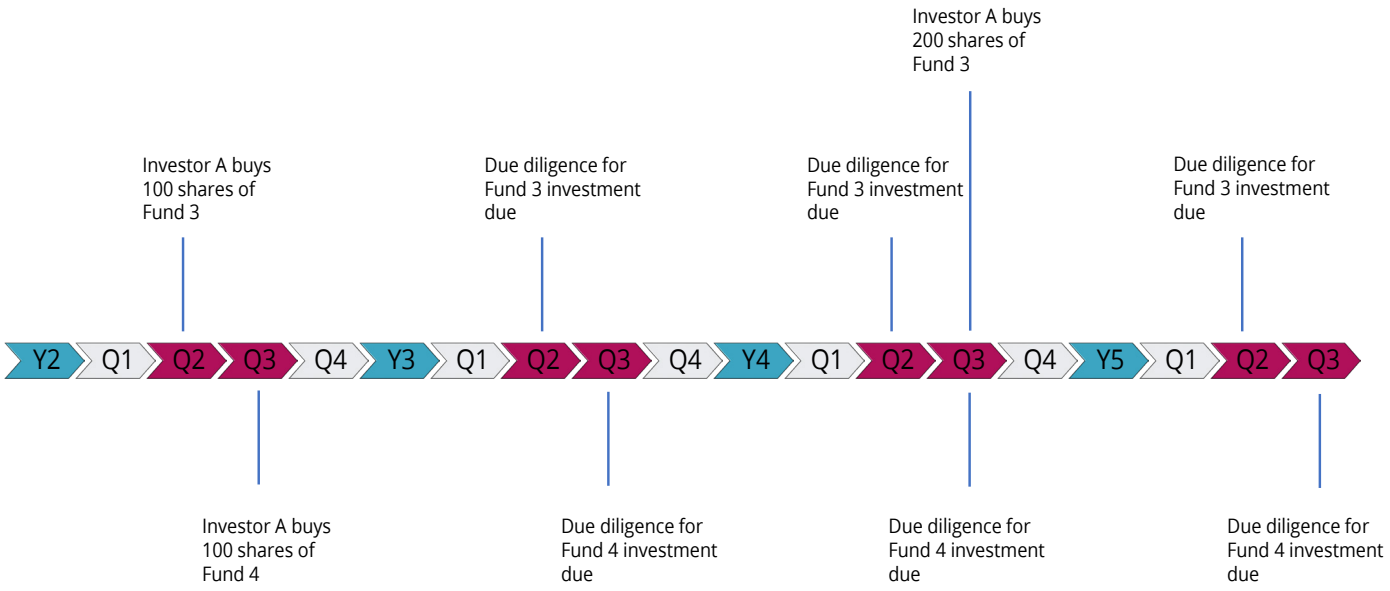
Under current requirements, entities such as fund administrators which perform due diligence for funds and investment managers on an outsourced/delegated basis are required to perform CDD separately for each fund regardless of any overlapping investors. Figure 5 below illustrates this:

Figure 5

Regulated Entity I



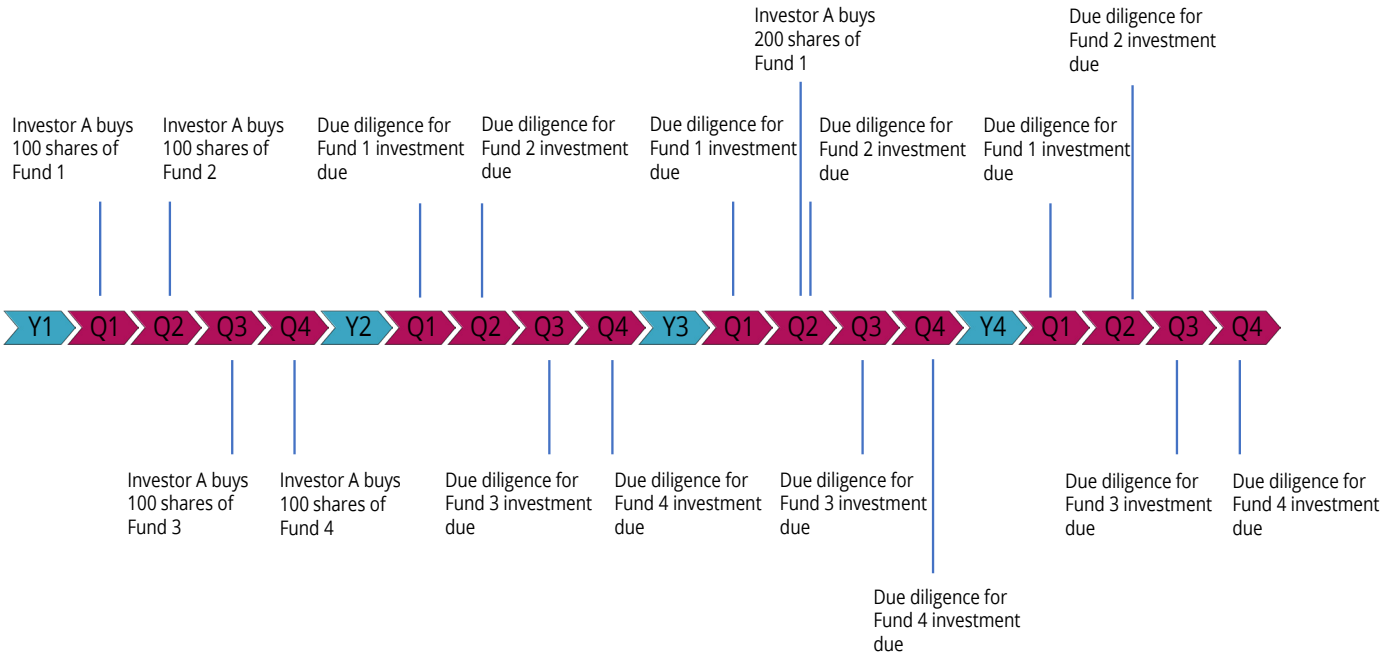
Regulated Entity II



20 We note that this option is already being utilised in practice by some fund administrators who have incorporated it through subscription agreements and the use of GDPR privacy notifications.

Fund administrators, in general, are not permitted currently to pool their efforts on behalf of one fund/investment manager with efforts on behalf of another fund/investment manager. So, an investor with investments in funds administered by the same fund administrator will be subject to multiple sets of CDD requests from the same fund administrator with potentially differing and overlapping timeframes. Figure 6 below illustrates this in a single sequential sequence:

Figure 6



However, if the fund administrator were able to apply pooled effort in the manner described in either of the variations discussed in Option 1 across the funds and investment managers it services, the CDD hits for the investor could be reduced from the 14 shown in Figure 5 to either 4 in the case of Variation A or 8 in the case of Variation B as shown in Figures 7 and 8.

Either of these variations would provide the following benefits, without any fundamental loss of CDD protection:

1. The investor would be subject to substantially fewer documentation requests; and
2. The fund administrator's CDD process could be streamlined resulting in potential cost savings that could be passed along to investors.

Challenges to overcome with this option include the need to be able to identify records attributable to each individual fund (and provide them separately upon request), the need to allow for oversight of the outsourced/delegated process and the need to overcome potential liability issues that may arise between the fund administrator and the investment manager.[21] This option would also introduce possible challenges with regards to the sharing or storing of these records under GDPR or other data protection restrictions that may exist in other jurisdictions.

21 For example, it may be the case that if a fund administrator is not acting as an administrator for all of the funds to which the investor is investing in, the administrator may be concerned about (potential) liability issues that may arise. The fund administrator may then want to enter into a relationship with the relevant investment manager which could cause commercial issues with any incumbent administrator.

Figure 7

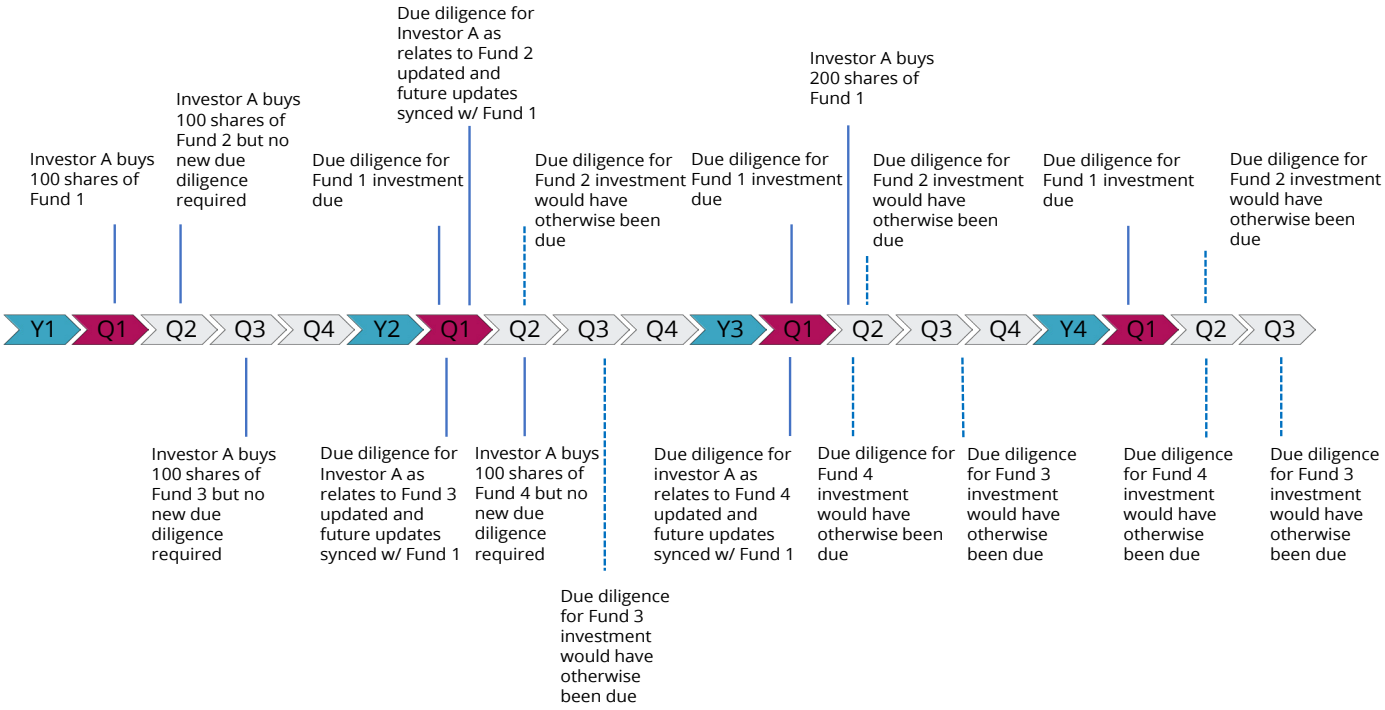
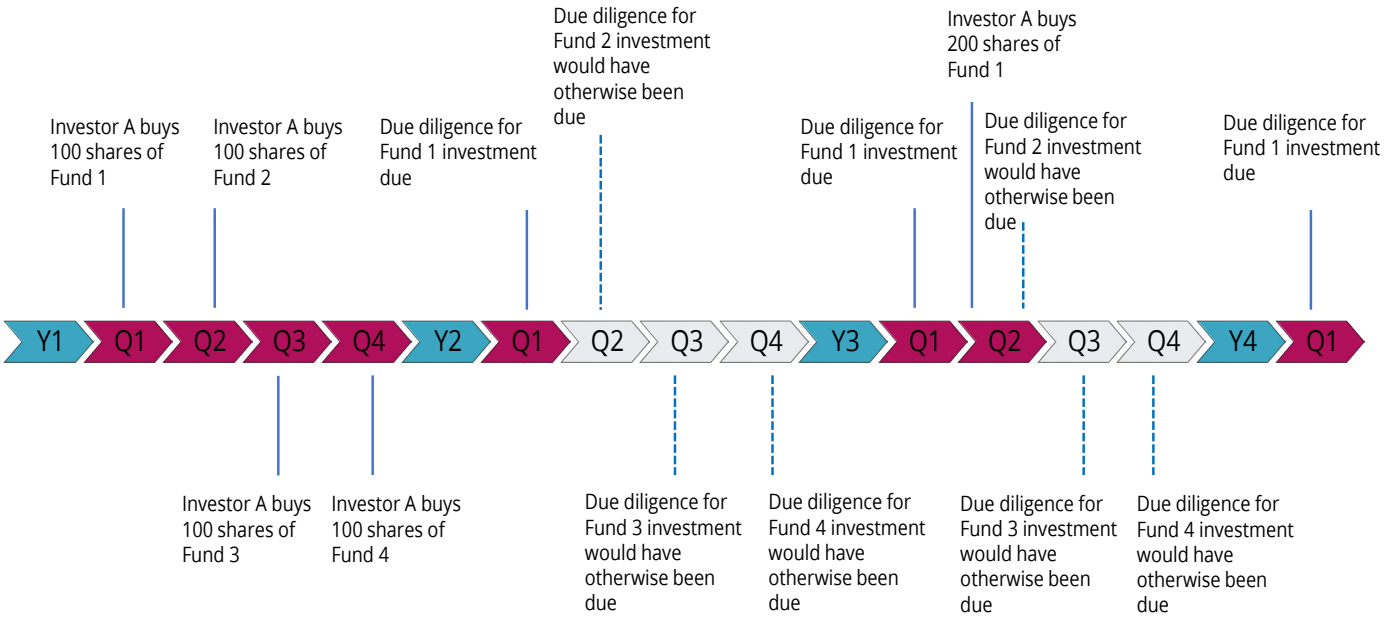


Figure 8



Option 3: Allow a regulated entity to perform due diligence for others on a reliance basis with regard to the requirements of a single country

A further improvement on options 1 and 2, and best operated in conjunction with those options, would be to establish a new regulated activity category for entities (i.e., a third-party provider), perhaps under MiFID (although changes to the list of regulated activities would need to be made), to perform CDD centrally and on a reliance basis for other regulated entities. For ease of reference, in this paper, we refer to these entities as "centralised due diligence processors" or "CDDPs".

Key aspects of this concept would include:

1. The CDDP would be required to be authorised to perform the functions of a CDDP, which would encompass all of the CDD requirements for regulated entities in that country, as well as specialised recordkeeping, operational resilience and cyber requirements due to the centralisation of these functions.

2. Regulated entities in scope of a country's AML/KYC/CTF requirements would remain subject to those obligations but could choose to employ a CDDP. If a CDDP was employed to perform the CDD functions, the other regulated entity could rely on the CDD performed by the CDDP subject to a periodic obligation to enquire regarding the continued good standing of each individual or entity on whom the CDDP had performed the CDD, unless the regulated entity had knowledge of any red flags suggesting that the conclusion reached by the CDDP was incorrect (in which case the regulated entity would need to complete the CDD process itself).

3. For any individual or entity with respect to which the CDDP had not performed CDD, the existing current requirements would still apply to the regulated entity. The regulated entity would also remain responsible for the other aspects of the AML/KYC/CTF programme such as suspicious activity reporting, etc.

4. The relying regulated entity would not be required to treat the CDDP as an outsourced service provider as the CDDP would be subject to the direct supervision of the relevant country's regulator.

This option would provide the following additional benefits:

1. The investor would be subject to even fewer documentation requests;

2. The substantial cost savings of not having multiple entities having to perform CDD on the same individual/entity could be passed along to investors;

3. The underlying obligations on regulated entities would remain as a backstop; and

4. Since the regulator will be directly supervising the CDDP, there can be closer supervision of the direct workings of the CDD and less variation in approach taken and judgment calls applied as fewer entities will be involved.

The recently published FATF Guidance provides guidelines for government authorities, regulated entities and other relevant parties to determine whether a digital ID is appropriate to use for customer identification and verification when onboarding investors. The FATF Guidance introduces, among others, the concept of an IDSP (i.e., CDDP) who operate as third-party entities in performing CDD on behalf of the investor.

Challenges to overcome with this option include the need to be able to identify records attributable to each individual fund, the change in the law needed to establish the CDDP category of regulated entities and to establish the parameters pursuant to which reliance by other regulated entities would be permitted. In addition, this option will also need to overcome any challenges related to potential liability issues that may arise between the CDDP and the fund administrator and the investment manager and challenges with regards to the sharing or storing of these records under GDPR or other data protection restrictions that may exist in other jurisdictions. Finally, the parties involved will have to agree on the fees/costs involved and who would be required to pay these.

The CDDP would also need to have strong data privacy and cybersecurity/data protection controls and the reliance on third parties may be acceptable for initial onboarding by some countries but may not be allowed for ongoing monitoring and the (annual) refresh cycle.

However, we note that FATF Recommendation 17 allows countries to permit regulated entities to rely on third parties to perform customer identification/verification when onboarding, provided that:

1. "The third party must also be a regulated entity subject to [CDD] requirements in line with Recommendation 10, and regulated and supervised or monitored for compliance;
2. The investment manager:
    a. Immediately obtains the necessary information concerning the identity of the investor (including the assurance (confidence) levels, where applicable; and
    b. Takes adequate steps to satisfy itself that the third party will make available copies or other appropriate forms of access to the identity evidence relating to Recommendation 10a[22] requirements upon request without delay."

Furthermore, relying on third party entities – whether they are fund administrators or CDDPs – to conduct customer identification/verification when onboarding is already allowed under Article 25 of the EU's Fourth Anti-Money Laundering Directive.[23] The fund, however, remains ultimately liable for any failure to comply notwithstanding its reliance on a third party.

Although this option would not necessarily have to result in a small number of CDDPs emerging, it may be that over time only certain types of business models would be able to support this, resulting in relatively small numbers of CDDPs. However, we are also not suggesting that the use of a CDDP should be mandatory, and financial services entities would still be free to comply directly with the CDD requirements without relying on a CDDP.

Option 4: Allow a regulated entity to perform due diligence for others on a reliance basis with regard to the requirements of multiple countries

Once the CDDP category is established, allowing CDDPs to seek authorisation from multiple countries (making them multi-country centralised due diligence processors or "MCDDPs" for ease of reference) to perform centralised CDD for regulated entities in those members states would be a logical extension. Although the MCDDP would be required to comply with the specific requirements and interpretations of multiple countries, provided options 1 and 2 were also in place, compliance could be relatively easily achieved through compliance with the most stringent standards of the relevant countries.

In this option, regulatory access would not be restricted, while efficiency would be further increased for investors and regulated entities using this facility.

This option builds on the basic digital ID ecosystem and its participants, as envisioned by the FATF Guidance,[24] by creating a standardised digital identity framework which allows MCDDPs to work across different jurisdictions.[25]

22 Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.

23 Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

24 See Appendix A of the FATF Guidance.

25 We also refer to a resolution, published by the European Parliament's Committee on Economic Affairs on 8 October 2020, which requests that the European Commission consider a framework for digital onboarding and the use of digital financial identities which would aim to harmonise these measures across the European Union. See https://www.europarl.europa.eu/doceo/document/TA-9-2020-0265_EN.pdf.

The FATF Guidance introduces a framework consisting of the three following components:

1. Identity proofing and enrolment (with initial binding/credentialing) (essential);
2. Authentication and identity lifecycle management (essential); and
3. Portability and interoperability mechanisms (optional).

Identity proofing answers the question, "Who are you?" and refers to the process by which an IDSP (i.e., (M)CDDP) collects, validates and verifies information about a person and resolves it to a unique individual within a given population or context. The second component, authentication, answers the question, "Are you the identified/verified individual?" and establishes whether the individual seeking to access an account (or other services or resources) — the investor — is the same person who has been identity proofed and enrolled. The IDSP confirms the validity of the CDD documentation with the investor and provides an authentication assertion to the financial institution.

The third component introduces the concept of a portable investor identity. According to the FATF Guidance, this concept "means that an individual's digital ID credentials can be used to prove official identity for new customer relationships at unrelated private sector or government entities, without their having to obtain and verify personal data and conduct customer identification/verification each time."[26] Options 3a/4a explore the framework in which (M)CDDPs can issue portable IDs and provide ongoing CDD lifecycle management on behalf of investors through the use of a digital solution.

Challenges to overcome with this option, and in line with the challenges identified under Option 3, include the need to be able to identify records attributable to each individual fund and the change in the law needed to establish the MCDDP category of regulated entities and to establish the parameters pursuant to which reliance by other regulated entities would be permitted. In addition, this option will also need to overcome any challenges related to potential liability issues that may arise between the MCDDP and the fund administrator and the investment manager and any challenges with regards to the sharing or storing of these records under GDPR or other data protection restrictions that may exist in other jurisdictions. The parties involved will have to agree on the fees/costs involved and who would be required to pay these. Finally, the reliance on third parties may be acceptable for initial onboarding by some countries or jurisdictions but may not be allowed for ongoing monitoring and the (annual) refresh cycle.

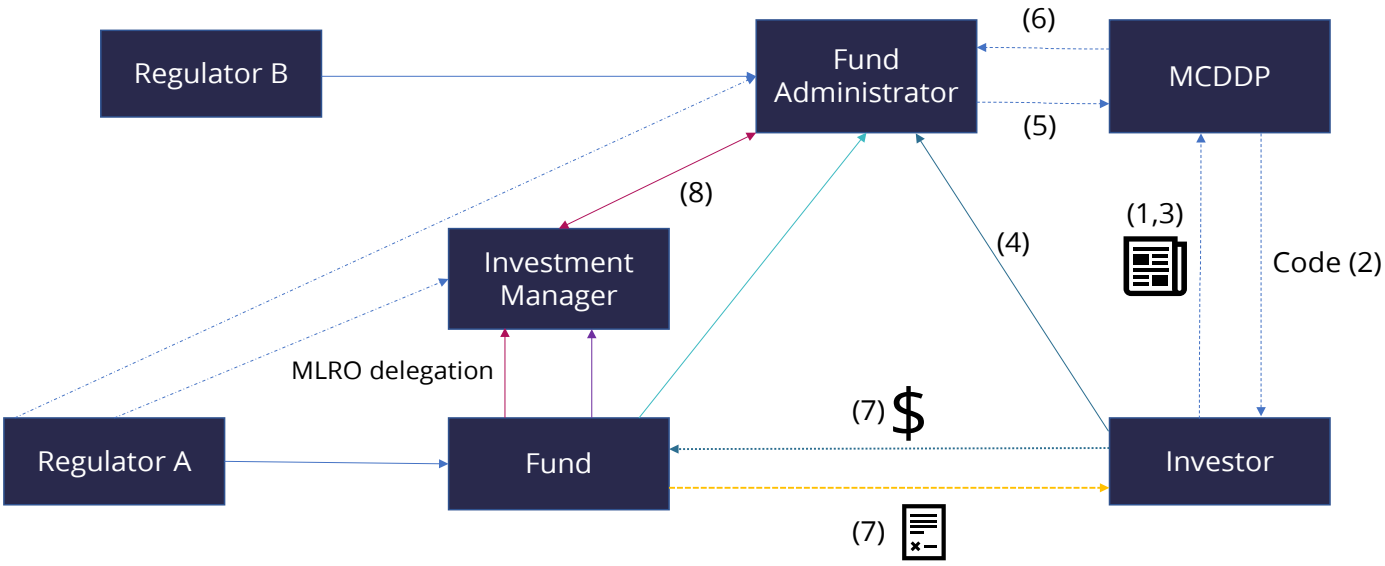
Option 3a/4a: Use a digital solution to amplify Option 3 or Option 4

The CDD process is a classic use case for a digital solution. Our suggestion, and in line with the FATF's introduction of a portable ID, is to create a portable digital identity framework centred with the MCDDPs. This framework would allow a third-party entity that has been authorised by the relevant regulator(s) to perform CDD on behalf of regulated entities (i.e., fund administrator/fund) and upon successful completion of the CDD, the investor's credentials can be used at other regulated entities without any additional lengthy CDD checks.

Our suggestion, however, would be to expand the framework by issuing the investor with a unique identifier code once it has successfully passed the CDD checks. It can then, through the MCDDP, provide the code to the fund as part of its subscription process. This would eliminate the need for a multitude of individual CDD checks having to be performed. The diagram below, which expands on Figure 1, and the accompanying explanatory notes, shows how this would change the flow of information and diligence.

26 See paragraph 69 of the FATF Guidance.

Figure 9



Notes:

(1) To start the process, the investor would open an account with the MCDDP (which could include a periodic service fee), selecting the jurisdictions for which the investor is seeking a digital identity clearance. These would have to include clearance with respect to the rules of Regulator A and Regulator B to purchase shares or units of the fund in this example. The investor would provide the required CDD documentation to the MCDDP.

(2) Once the MCDDP had completed its processing and CDD, the investor would be provided with a digital identity clearance code.

(3) Upon receiving the digital identity clearance code, the investor would then identify for the MCDDP which financial services entities should have the ability to seek verification from the MCDDP. To maintain the ability to allow these verifications, the investor would have to provide the necessary CDD updating documentation in a timely manner so that the MCDDP could update its CDD periodically. If the investor were to fail the ongoing CDD (or decided to cancel its account with the MCDDP), the digital identity verification code could be deactivated by the MCDDP.

(4) The investor would provide the digital identity code to the fund administrator as part of the subscription process.

(5) When the fund administrator in receipt of the digital identity code would still have a CDD obligation under the law (in this example the relevant law being the rules of both Regulator A and Regulator B) but this could be satisfied in the alternative to the normal method by submitting the digital identity code back to the MCDDP to seek verification of currently effective CDD clearance. This process would be repeated then periodically as the fund administrator's regular CDD cycle would require.

(6) Assuming the investor is in good standing with the MCDDP and has cleared the CDD process as well as any relevant interim CDD updates, the MCDDP would send back a verification to the fund administrator which could be relied on until the date indicated in the verification by the MCDDP. If the investor cancelled its account with the MCDDP or failed the ongoing CDD, the MCDDP would be authorised to inform any regulated entity to which it had provided a verification that the MCDDP was no longer standing behind the verification, putting the CDD obligation back on the other regulated entity as normal.

(7) Only after the verification was obtained from the MCDDP (or the necessary CDD is otherwise performed by the fund administrator) would the fund be permitted to accept the funds from the investor and issue the relevant number of shares/units in return.

Recommendation 17, as mentioned above, could be expanded to explicitly include the generation and assignment of a digital ID – through a digital identity clearance code – to an investor or its legal

representative or enable the verification and sharing of the investor's attributes. We note that this concept has been explored to a greater or lesser degree by other market participants. For example, IHS Markit, a global information provider, has created an interactive digital platform[27] to collect, manage, request and store investors' KYC information. The platform provides a CDD workflow process for all market participants involved in the fund industry, including investors. The platform supports bilateral exchange with clients and simplifies and enhances CDD through a secure, centralised environment. Another example is an organisation called The ID Register which provides investors the opportunity to create their own online CDD profile through which they can upload all necessary documents.[28] The ID Register then proceeds to verify these IDs and assesses the risk-level investors present. Every profile is authenticated and vetted against global sanctions and PEP lists and kept up to date by real-time sanctions screening.

As per the steps outlined above, the investment manager would only be obligated to perform the minimum amount of CDD checks. The investor retains complete control of his/her information and can tailor the information it wants to share to the need of the party requesting it. With wide adoption, funds will only need to require the investor's code as part of their subscription questionnaires. This means there will be consistency across their portfolios and a reduction in the time and effort required to fill out subscription documents. Challenges to overcome with this option, and in line with the challenges identified under Options 3 and 4, include the need to be able to identify records attributable to each individual fund and the change in the law needed to establish the MCDDP category of regulated entities and to establish the parameters pursuant to which reliance by other regulated entities would be permitted. In addition, this option will also need to overcome any challenges related to potential liability issues that may arise between the MCDDP and the fund administrator and the investment manager, challenges with regards to the sharing or storing of these records under GDPR or other data protection restrictions that may exist in other jurisdictions. The parties involved will have to agree on the fees/costs involved and who would be required to pay these. Finally, the reliance on third parties may be acceptable for initial onboarding by some countries or jurisdictions but may not be allowed for ongoing monitoring and the (annual) refresh cycle.

An aside

Although this paper is focused on CDD, the concepts raised here could also usefully be applied to other areas of eligibility determinations, such as assessments about whether an investor is a "professional client" under the requirements of Annex II of MIFID.

Considerations for standard setters

(Portable) digital IDs must be properly embedded into CDD frameworks and simply adding a Recommendation or an article to existing regulation is not enough to provide the necessary clarity. Participants will need to consider carefully the operational and legal requirements that will need to be adopted before the above listed options could be implemented. As mentioned throughout this paper, GDPR and other data protection restrictions may prevent the complete and successful implementation of any of the options listed above. However, these could potentially be resolved by allowing for the sharing of (personal) investor data which could be agreed on through subscription agreements.

Regulators may also be constrained in allowing (M)CDDPs to perform their activities due to legal national and regional limitations on the use of third-party entities. However, we note that these obstacles could be overcome through the agreement and recognition of (M)CDDPs between regulators. In this respect, we refer to the EU's eIDAS framework which provides a common legal framework for the cross-border recognition of electronic ID schemes across the EU.[29] In the United States, the NIST Digital Identity

27 IHS Markit Investor Access, see https://ihsmarkit.com/products/kyc-services.html.

28 The ID Register, see https://www.theidregister.com/services/kyc/.

29 Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market. The European Commission announced its intention to improve the eIDAS framework by extending its application to the private sector and by promoting trusted digital identities throughout the EU. See European Commission Communication on a Digital Finance Strategy of the EU, available as of 24 September 2020 at https://ec.europa.eu/transparency/regdoc/rep/1/2020/EN/COM-2020-591-F1-EN-MAIN-PART-1.PDF.

Guidelines[30] provide technical requirements for federal agencies implementing digital ID services and cover identity proofing and authentication of users interacting with U.S. government IT systems. In the United Kingdom, electronic identification through documents or information obtained from a reliable source is now allowed for CDD purposes. The information, however, must be obtained by means of an electronic identification process and the process must be secure from fraud and misuse and capable of providing an appropriate level of assurance that the person claiming a particular identity is in fact the person with that identity.[31] The scope of the EU and U.S. frameworks could be expanded to include CDD and other jurisdictions could request to join or, alternatively, could replicate an identical regime which would increase the adoption of cross-border investor CDD.

Regulators' reliance on each other's frameworks enables jurisdictions to accommodate different national requirements, provided that the outcome is compliant with a pre-determined set of minimum standards. In order for the options to work as intended, regulators should promote close cooperation between the public and private sector and encourage a harmonised and interoperable ecosystem, without requiring individual (M)CDDPs or other regulated entities pooling their resources to seek approval and endorsement in separate jurisdictions. This can be achieved by endorsing (M)CDDPs and its activities while providing close regulatory oversight. Regulators will need to agree on standards and principles, including on the aspects of identity that determine what forms of digital ID are acceptable and the type of verification methods that provide an acceptable level of assurance.

The following questions have their basis in regulatory, often operational and unintentional hurdles that transposition of the above digital ecosystem can present and need to be fully considered before its implementation.

Data protection

- Could investors withdraw their permission for sharing the alphanumerical code?
- Who would be liable for potential data loss, data corruption or misuse of data due to unauthorised access?
- To what extent is the investment manager liable if the information it relies on turned out to be false or misleading?
- Who would be liable if the personal identifiable information of an investor is "erased or rectified without delay"?

Cybersecurity

- What appropriate, technology-based safeguards, as well as effective governance and accountability measures need to be in place to prevent potential cyber breaches?

Operational considerations

- Would it be voluntary or mandatory for the investors?
- Would it be voluntary or mandatory for investment managers, fund administrators and other financial services providers?
- What would be the costs involved, who would pay these costs?
- Could investors withdraw their permission for sharing the number?
- What happens if the investor fails to update paperwork or otherwise is deemed to fail checks? How would financial service providers be notified and what would they be required to do about it?
- Are all parties involved confident they have the right operational and risk management requirements in place to ensure full compliance with its (legal) obligations?

We hope that the proposal as outlined above will be helpful. We would be happy to discuss further any of the suggestions raised in this paper.

30 See https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

31 Regulation 28(18)(19) of the Money Laundering and Terrorist Financing (Amendment) Regulations 2019.

APPENDIX A

Summary of options

Options	Core Assumption	Benefits	Challenges
Option 1	Regulated entity to pool CDD efforts within own organisation	1. The investor would be subject to substantially fewer documentation requests; 2. The regulated entity's CDD process could be streamlined; and 3. The CDD results with respect to each individual investor investing in separate funds would provide greater regulatory oversight for regulators.	1. Need to identify records attributable to each individual fund; and 2. Possible restrictions of the sharing of records under GDPR or other data protection regulations
Option 2	Regulated entity performing CDD for others on an outsourced/ delelegated basis to pool CDD efforts	1. The investor would be subject to substantially fewer documentation requests; and 2. The fund administrator's CDD process could be streamlined resulting in a potential cost savings that could be passed along to investors;	1. Need to identify records attributable to each individual fund; and 2. Allow for oversight of outsourced/delegated process; and 3. Possible restrictions of the sharing of records under GDPR or other data protection regulations.

Options	Core Assumption	Benefits	Challenges
Option 3	Regulated entity performing CDD for others on a reliance basis with regard to single country requirements	1. The investor would be subject to even fewer documentation requests; 2. The substantial cost savings of not having multiple entities having to perform CDD on the same individual/entity could be passed along to investors; 3. The underlying obligations on regulated entities would remain as a backstop; and 4. Since the regulator will be directly supervising the CDDP, there can be closer supervision of the direct workings of the CDD and less variation in approach taken and judgment calls applied as fewer entities will be involved.	1. Need to identify records attributable to each individual fund; 2. Change in law needed to establish the CDDP category; 3. Establish parameters to which reliance by other regulated entities would be permitted; 4. Potential liability issues that may arise between the CDDP and the fund administrator and the investment manager; 5. Possible restrictions of the sharing of records under GDPR or other data protection regulations; 6. Agreement must be reached on the fees/costs involved and who is required to pay these; and 7. Reliance on third parties may be acceptable for initial onboarding by some countries or jurisdictions but may not be allowed for ongoing monitoring and the (annual) refresh cycle.
Option 4	Regulated entity to perform CDD for others on a reliance basis with regard to multiple country requirements	1. The investor would be subject to even fewer documentation requests; 2. The substantial cost savings of not having multiple entities having to perform CDD on the same individual/entity could be passed along to investors 3. The underlying obligations on regulated entities would remain as a backstop; and 4. Since the regulator will be directly supervising the MCDDP, there can be closer supervision of the direct workings of the due diligence and less variation in approach taken and judgment calls applied as fewer entities will be involved.	1. Need to identify records attributable to each individual fund; 2. Change in law needed to establish the (M)CDDP category; 3. Establish parameters to which reliance by other regulated entities would be permitted; 4. Potential liability issues that may arise between the CDDP and the fund administrator and the investment manager; 5. Possible restrictions of the sharing of records under GDPR or other data protection regulations; 6. Agreement must be reached on the fees/costs involved and who is required to pay these; and 7. Reliance on third parties may be acceptable for initial onboarding by some countries or jurisdictions but may not be allowed for ongoing monitoring and the (annual) refresh cycle.

Options	Core Assumption	Benefits	Challenges
Option 3a/4a	Use a FinTech solution to amplify Option 3 or Option 4	1. The investor would be subject to even fewer documentation requests; 2. The substantial cost savings of not having multiple entities having to perform CDD on the same individual/entity could be passed along to investors; 3. The underlying obligations on regulated entities would remain as a backstop; 4. Since the regulator will be directly supervising the (M) CDDP, there can be closer supervision of the direct workings of the CDD and less variation in approach taken and judgment calls applied as fewer entities will be involved; and 5. The investor retains complete control of his/her information and tailors the information he/she wants to share with the entity requesting it.	1. Need to identify records attributable to each individual fund; 2. Change in law needed to establish the (M)CDDP category; 3. Establish parameters to which reliance by other regulated entities would be permitted; 4. Potential liability issues that may arise between the (M)CDDP and the fund administrator and the investment manager; 5. Possible restrictions of the sharing of records under GDPR or other data protection regulations; 6. Agreement must be reached on the fees/costs involved and who is required to pay these; 7. Consideration needs to be given to operational, cybersecurity and data protection implications of this option; and 8. Reliance on third parties may be acceptable for initial onboarding by some countries or jurisdictions but may not be allowed for ongoing monitoring and the (annual) refresh cycle.

www.aima.org