BDO

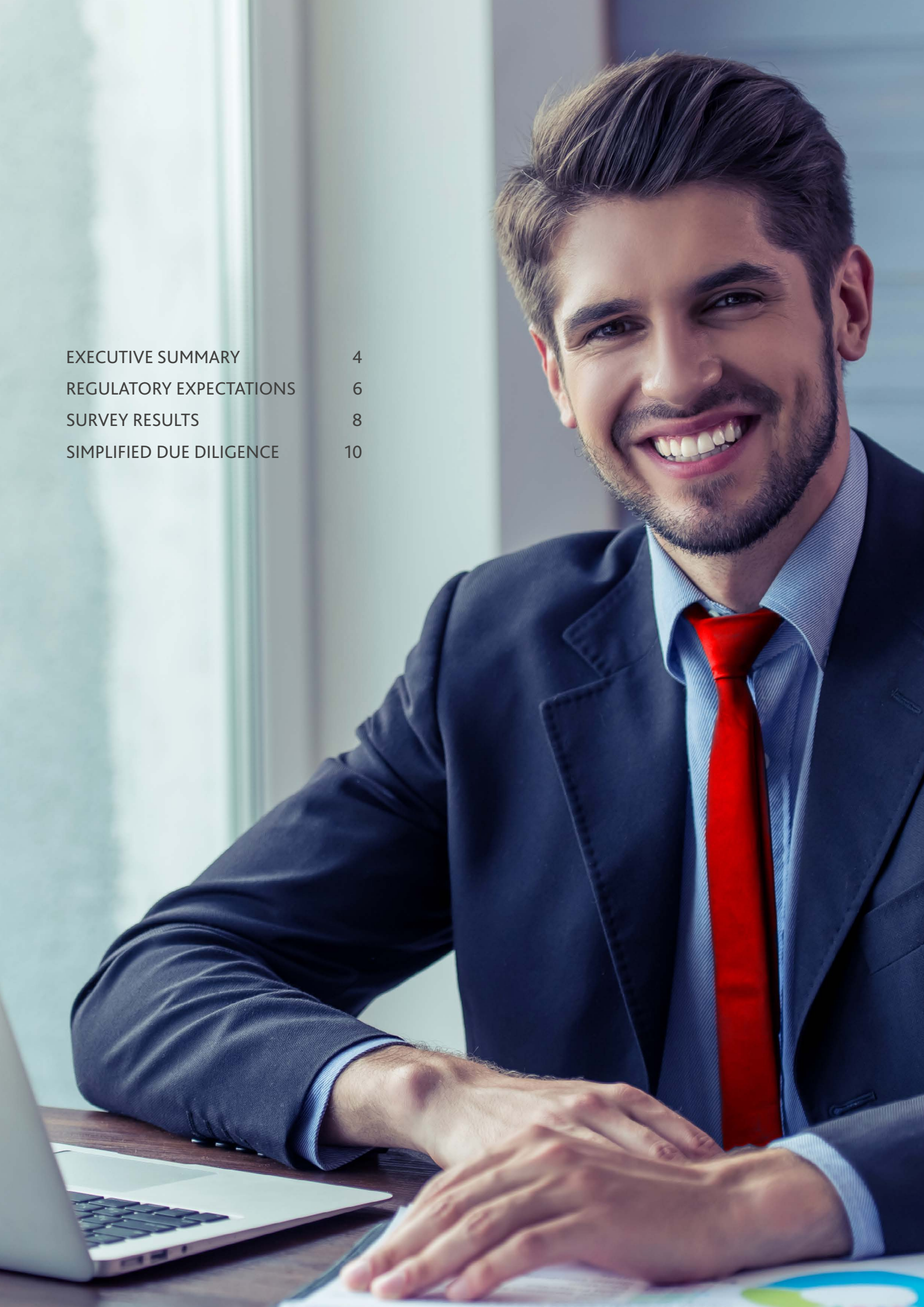
IDEAS | PEOPLE | TRUST

ASSOCIATION OF FOREIGN BANKS

WHEN DID SIMPLIFIED DUE DILIGENCE BECOME NOT SO SIMPLE?

# SIMPLIFIED DUE DILIGENCE

JULY 2019



I am delighted to set out the following Simplified Due Diligence ('SDD') report which BDO, the Association of Foreign Banks and its members have collaborated to produce.

For a number of years, regulated firms have conducted SDD on clients who are deemed to be lower risk, mainly due to the transparency of their legal entity type; in particular, regulated institutions and publicly listed companies.

When the European Commission published the 'Fourth Money Laundering Directive' (4MLD) in 2015, regulated firms' eyes were drawn to the change in SDD. Firms are no longer permitted to apply a blanket approach to SDD. This is a significant change for firms… or is it? Nowhere in the Money Laundering Regulations 2017 (MLR 2017) does it say that industry is not allowed to continue using SDD as an effective means to on-board or monitor client relationships. In fact, Regulation 37 specifically provides relevant persons directions on when SDD is applicable.

However, as the results of the survey shows, a number of banks have given up on SDD. Is this due to a misunderstanding of what the regulations are trying to achieve? Or is it because regulated institutions are too concerned about what limited due diligence might bring, the expensive wrath of the regulator and social opinion?

This report seeks to provide a snap shot of what banks are currently doing in the context of SDD, and more importantly, to bridge the gap between regulation and best practice, and shed some much-needed light what banks should be doing to fulfil their SDD obligations.

Yours sincerely

**FIONA RAISTRICK**

**Partner, Financial Services Advisory**
**For and on behalf of BDO LLP**

It is a great privilege for the Association of Foreign Banks (AFB) to collaborate with BDO on a hot topic within the sphere of financial crime prevention and provide a helpful analysis for the benefit of our broad membership of c.200 international banking groups operating in the UK.

The AFB's Policy work on financial crime has grown significantly in the last 12 months, bifurcating the once single Financial Crime Committee into three, thematically organised, discussion groups that gather MLROs and financial crime practitioners on a quarterly basis to address issues across: AML/CTF; Anti-bribery, Sanctions & Fraud; and Cybercrime & Cryptocurrencies.

Since I joined the Board of the JMLSG at the end of 2018, the AFB has also grown its efforts to evolve the industry's Guidance and, where appropriate, cavass its membership on processes to help share best practices and support improvements in compliance to relevant regulations. This paper is a great collaborative project with BDO's specialists to shed light on Simplified Due Diligence which, following receipt of views from over 30 inbound firms, is not as simple as once expected.

Finally, I'd like to thank James Leigh, Senior Associate, in my team for supporting me on this project. We hope you find this paper to be useful and would welcome feedback on any other areas of financial crime for which the AFB can develop insight.

Yours sincerely

**BRUK WOLDEGABREIL**

**Director, Association of Foreign Banks**

# EXECUTIVE SUMMARY

## BACKGROUND

The Association of Foreign Banks (AFB), earlier this year, received a query from the Editorial Panel of the Joint Money Laundering Steering Group (JMLSG) regarding how regulated firms currently undertake Simplified Due Diligence (SDD) in compliance with the Fourth Money Laundering Directive (4MLD). The Editorial Panel was keen to have this insight to help shape the current JMLSG Guidance to better reflect the realities of SDD post-4MLD implementation.

The AFB created a succinct four question survey for its members to capture the latest thinking with respect to SDD processes in practice. The four questions were:

**01** Are you still applying SDD to other equivalently regulated Financial Institutions?

**02** If so, what criteria do you use in assessing whether such Financial Institutions pose a low Money Laundering / Terrorist Financing risk?

**03** What does SDD actually look like in your firm, for example: what due diligence measures are being undertaken?

**04** Are there other client types, aside from Financial Institutions, to which SDD is currently being applied to?

The AFB received 32 responses – 13 from EEA banks and 19 from non-EEA banks. BDO was invited to analyse the results and provide regulatory and industry best practice on how banks should approach SDD.

## KEY FINDINGS

- Over 20% of respondents indicated that they no longer apply SDD to other equivalently regulated Financial Institutions (FIs)
- EEA banks feel less comfortable in conducting SDD, with more stating they no longer apply SDD
- 34% of respondents that do still apply SDD only assess two factors when determining the applicability of SDD rather than undertaking a holistic customer risk assessment
- Almost 90% of respondents noted 'country risk' as a key factor when considering if SDD is appropriate
- Over 50% of respondents state that PEP, sanctions and adverse media screening on the customer plays a key role in assessing the customer as low risk
- 10% of respondents are not identifying the customer's beneficial owners when applying SDD, a breach of MLR 2017
- Whilst all respondents broadly understood that SDD represents a loosened form of Customer Due Diligence (CDD) rather than an exemption from it, the results showed a substantial disparity of approach in what information and/or documentation banks collect when conducting SDD. This suggests that, in practice, there is uncertainty amongst the banking community as to what SDD truly means.

## CONCLUSION

A bank's AML framework must be built on its size, business model and complexity. The results of its enterprise-wide risk assessment (EWRA) should then inform the systems and controls. Therefore, from a survey of 32 banks, it is not surprising to see 32 very different results. There are similarities of course, the results showed consistent approaches regarding assessing 'country risk' when deciding whether SDD was applicable. It's also not surprising that a few firms no longer utilise SDD as a control. Banks are under a huge amount of scrutiny and so they are concerned about the level of due diligence they are conducting.

Although there are multiple components of a financial crime framework, there is always a big emphasis on a firm's due diligence processes and controls. Of course governance, your risk assessment, data management are all key to assisting you in mitigating money laundering and terrorist financing risk, but if your CDD is stringent and robust enough, then this goes a long way in cutting off criminals from entering the UK financial system.

4MLD and the MLR 2017 signalled a shift in the SDD paradigm – the Directive and 2017 legislation sought to further emphasise the importance of assessing risk, and avoiding a tick-box approach, even in the context of customer relationships which were low risk.

What is obvious is that the FCA wants all relevant persons to have strong AML frameworks.

They want banks to take responsibility for their risks, evaluate the threats that each customer relationship holds, and apply a proportionate risk-based approach to their due diligence, which doesn't comprise control.

Therefore, SDD is an important and valuable tool for banks. The FCA are consistently encouraging regulated institutions to take a risk based approach, not only with its AML framework, but also its CDD. Legislation requires banks to conduct Enhanced Due Diligence (EDD) on its customers, when a client poses higher inherent risks. The MLR 2017 states that further information be sought and be verified when such clients are on-boarded.

In the same way which the FCA expects banks to conduct EDD on high risk clients, the FCA expects firms to conduct SDD on low risk clients. If performed well, and to the standard expected by the Regulator, SDD can assist in an effective and efficient risk based approach due diligence process.

# REGULATORY EXPECTATIONS

## What does regulation and industry guidance say about SDD?

### INTERNATIONAL CONTEXT

The Financial Action Task Force ('FATF') recommendations are seen globally as the gold standard in Money Laundering and Terrorist Financing preventative measures.

The Interpretive note to the Recommendation 10 (which establishes the requirement to apply Customer Due Diligence measures) states that:

> "Where the risks of money laundering or terrorist financing are lower, financial institutions could be allowed to conduct simplified CDD measures, which should take into account the nature of the lower risk. The simplified measures should be commensurate with the lower risk factors.

### MOVING FROM '3MLD' TO '4MLD'- LOSING THE 'BLANKET EXEMPTION'

4MLD removed the so-called 'blanket exemption' or carte blanche (previously applicable under 3MLD) whereby SDD could be applied to a prescribed list of customer types (generally speaking – customers who are regulated entities in their own right).

Instead, 4MLD governed that firms would need to determine the level of risk posed by a customer prior to applying SDD and provide a rationale and justification for it.

Annex II of 4MLD includes a non-exhaustive list of factors and types of evidence of potentially lower risk, which could be used to determine whether SDD is applicable.

### MLR 2017

On 26th June 2017, 4MLD was implemented into UK law through The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ('MLR 2017').

Regulations 27 and 28 provide the primary reference point for when and how firms should conduct CDD. Broadly, Regulation 28 states that such measures include:

- Identifying the customer and verifying their identity using documents and information from a reliable source which is independent of the person being verified
- Assessing and where appropriate obtaining information on the purpose and nature of the business relationship
- Where the customer is a body corporate – obtaining the corporate's name, company/registration number and registered office address and if different, its principal place of business (and verifying this information)
- Where the customer is a body corporate not listed on a regulated market, taking reasonable measures to identify and verify the law to which it is subject, its constitution and the full names of the board of directors (or equivalent management body) and the senior persons responsible for operations
- Identifying beneficial owners and taking reasonable steps to verify their identity.

Regulation 37 of the MLR 2017 specifically focuses on SDD, stating that:

> "A relevant person may apply simplified customer due diligence measures in relation to a particular business relationship or transaction if it determines that the business relationship or transaction presents a low degree of risk of money laundering and terrorist financing…

## JMLSG GUIDANCE

As with previous iterations of the MLRs, running parallel with the legislative provisions of the MLR 2017, is the guidance provided by the Joint Money Laundering Steering Group ('JMLSG').

The JMLSG guidance provides further information on what SDD measures could be applied, which include adjusting:

- The timing of CDD
- The quantity of information obtained for identification, verification, and monitoring
- The quality or source of information used for identification, verification and monitoring
- The frequency of CDD updates and reviews of the business relationship
- The frequency and intensity of transaction monitoring.

As an indicative example, Sections 5.3.136 – 5.3.138 of the JMLSG guidance state that:

> Applying simplified due diligence might involve:
>
> - Checking with the home country central bank or relevant supervisory body
> - Checking with another office, subsidiary, branch or correspondent bank in the same country
> - Checking with a regulated correspondent bank of the overseas institution
> - Obtaining from the relevant institution evidence of its licence or authorisation to conduct financial and/or banking business.

# SURVEY RESULTS

## What do the results say about the industry

> We no longer apply SDD to other equivalently regulated financial institutions due to the changes made by the 4th MLD.
>
> **SURVEY RESPONDENT**

### OVERVIEW

SDD is a regulatory due diligence tool for financial institutions to utilise when clients are deemed low risk. It is a paramount instrument to assist firms in having an effective and efficient on-boarding and ongoing monitoring process. However, in a time when financial institutions are under extreme regulatory scrutiny, firms feel less comfortable in applying SDD. Socio-economic impact is also leading to firms wanting 'to do the right thing' and combat financial crime. The gateway to the financial system is due diligence on banks' clients, therefore, the more due diligence you complete; then theoretically, the less likely it is that illicit funds will enter a bank, and the financial system.

### ARE BANKS STILL APPLYING SDD?

In short, 'yes'. With 78% of the respondents noting that their bank applies SDD measures when it is appropriate, using a risk based approach. However, this highlights that 22% are not applying SDD, even though the MLR 2017, specifically Regulation 37, allows it.

The survey shows that banks from the European Economic Area (EEA) feel less comfortable in conducting SDD than non-EEA banks.

Commentary from the respondents, suggests that changes brought about by 4MLD seem to be the primary factor for EEA banks moving away from SDD.

It is also clear that banks are only applying SDD to other financial institutions.

**What criteria are banks assessing when considering whether such clients pose a low money laundering risk?**

One of the major risk factors that banks are assessing when considering whether SDD is appropriate is 'country risk'. Of those banks who apply SDD, only 8% did not explicitly state that the jurisdiction of a client is part of the assessment to determine whether SDD is appropriate.

Further to 'country risk', a major factor that firms are assessing is customer screening. Almost 50% of respondents noted this as an important factor when deciding if SDD can be applied. Customer screening conducted on clients is:

1. Whether the client, or any connected parties (directors, senior management, UBOs) are politically exposed persons (PEPs)
2. Whether the client, or again connected parties, have any sanctions exposure
3. Lastly, whether the client or connected parties, has any relevant adverse media related to them.

Any positive hits on the points above, would, and should, rule out the application of SDD.

It is positive to see that the nature of the products and services offered, also appears to be significantly prevalent as criteria for determining the applicability of SDD. In the last five years, the threat assessment of activities such as trade finance and correspondent banking has rocketed. Previously, a correspondent banking relationship with another bank would be deemed as lower risk. The other bank is regulated, therefore they must be compliant. However, recent enforcement cases against a number of banks, highlights that the UK's financial institutions' AML systems and controls need improving.

Nowadays, where there is more social pressure on governments to deter the use of offshore companies to avoid tax, as well as evade it, it was surprising to see so few results note that a client's ownership structure complexity would negate the applicability of SDD. In fact, only two respondents noted this as a factor. Complex offshore structures are not only a way in which criminals evade tax, but also an important tool for criminals to hide their ownership, and ultimately the concealing of illicit funds.

Interestingly, one bank deemed that SDD would only be appropriate for financial institutions that are both regulated and listed. This has evolved from when a blanket approach was applicable in industry, when a bank could apply SDD to a regulated or listed company.

One bank deemed that its framework only currently permits SDD in relation to entities listed on approved stock exchanges or subsidiaries of such entities – i.e. SDD for unlisted regulated financial institutions is not currently in the scope of its procedures.

### Typical controls banks are using

All respondents appear to be broadly aware that SDD is not a de-facto exemption from conducting CDD, rather it represents a lesser extent of CDD. The majority appear to understand that Regulation 28 of MLR 2017 is still relevant.

However, over 10% of respondents are failing to identify the beneficial owners of a regulated customer, instead only focussing on obtaining proof of regulation and the address.

This is a breach of Regulation 37, which still requires banks to adhere to Regulation 28, and therefore obtain information on beneficial owners. E-money institutions (EMIs) are developing rapidly however they do not undergo the same scrutiny as banks, therefore banks should be aware that not all authorised EMIs would be assessed as low risk.

In some responses, likely to be banks with correspondent banking services, firms are obtaining other financial institution's AML policies and procedures and Wolfsberg Questionnaires. This process has been enhanced in recent years, and when a bank has such a relationship, a risk based approach should be taken to understand whether just obtaining the AML policies and procedures is sufficient. For higher risk correspondent banking relationships, banks are now going beyond just collecting AML policies and procedures, but testing the operational effectiveness of these policies.

Customer screening plays an important role in considering whether SDD is applicable to the client. It was therefore unsurprising to see so many results quote PEP, sanctions, and adverse media screening as relevant controls when applying SDD. However, what is difficult is understanding what is relevant negative news, and what can be deemed as 'unsubstantial' or 'historical'. For example, as mentioned earlier, a number of banks have been in trouble with the regulator for weakness of AML systems and controls. However, does this mean you should not be doing business with the majority of large UK banks? Probably not. What it does mean however, is the requirement to understand from your client, the progress they have made since the regulatory enforcement.

### Which other types of entities are banks applying SDD to?

Lastly, the survey also asked banks to note which other client types they would apply SDD to. Encouragingly, the majority correctly noted that "this will be done on a case-by-case basis" or "where the overall risk is assessed as low". However, over 50% responses still simply only stated varying legal entity types, such as:

- Listed companies (or companies majority owned by a listed company)
- Regulated funds
- Pension funds
- Public authorities
- State owned entities
- Low risk governments.

The above suggests that the blanket approach to SDD is still prevalent in the market. Although the legal entity type is important to assess when deliberating whether SDD is applicable, ultimately the overall risk has to be low.

### Why are banks not conducting SDD anymore?

There are four main answers. Firstly, that banks will only maintain relationships with other financial institutions in the context of products and services which are inherently high risk (such as Trade Finance and Correspondent Banking) and therefore SDD is never appropriate in such circumstances. Secondly it is easier to take a generic approach that SDD is not acceptable rather than having to assess whether each relationship is low risk enough.

However, the remaining two reasons are more concerning. One being, that in some cases there is a misunderstanding of the regulations. The removal of the "blanket approach" to SDD does not mean the removal of SDD altogether. In fact, one could argue that it gives banks more license to apply SDD to clients where previously it would not be deemed as applicable.

However, what is clear, not only from the survey, but also our expertise in the market working with a number of financial institutions, is that there is a fear of 'not doing enough'. As the US regulators have 'super-sized' their regulatory enforcements, not just the financial penalty, but then the cost of court appointed monitorships, so to has the FCA. The public have also become more aware of the financial crime crisis, and therefore are also applying pressure on banks to do more to hinder criminals accessing the financial system and growing predicate offences such as drug and human trafficking.

Pressure from governments, regulators and the public, should not mean that banks should abandon the perfectly acceptable regulatory method of SDD. What it does require though, is a robust customer risk assessment to firstly make sure the client is low risk, and then industry best practice SDD controls to make sure the due diligence sufficiently adheres to Regulation 28.

# SIMPLIFIED DUE DILIGENCE

## What does best practice look like?

The most fundamental building block of adopting a best practice approach to the application of SDD is for firms to be cognisant that simplified measures are not a one-size fits-all.

This section of our report comprises a collection of 'best practices' which we have compiled using industry and supervisor-led guidance, our Skilled Persons work, and the approaches which our portfolio of banking clients apply.

SDD is not a de-facto exemption from standard CDD measures. With this in mind, firms are expected to conduct a risk assessment prior to the application of simplified measures. The aim of this risk assessment is:

1. To determine whether a prospective customer's financial crime risk profile will allow for SDD to be applied
2. To determine the extent of the simplified measures, after establishing that SDD is sufficient, in order to adequately manage the low levels of financial crime risks identified

Despite the abundance of guidelines and best practice provisions such as the publications by the Joint Money Laundering Steering Group (JMLSG) and the European Banking Authority (EBA), many firms still face challenges in changing their old SDD habits and controls that were developed and embedded over a span of 10 years under the old regime.

### SIMPLIFIED DUE DILIGENCE ASSESSMENT FACTORS

Under the new regulatory regime, firms can no longer automatically apply simplified measures to a 'pre-defined' list of customers. Firms must be aware that customers cannot just meet pre-defined criteria in order to qualify for SDD.

Long gone are the days where firms can engage SDD measures simply because their customer is a legal entity with securities listed on a recognised exchange.

The expectation is now for firms to gather information and conduct a proportionate assessment of risk before determining whether a customer can qualify for SDD. By doing so, firms will satisfy themselves that the underlying risks associated with the customer or relationship are indeed low.

More often than not, firms with robust SDD arrangements will have a comprehensive and equally robust enterprise-wide assessment of the money laundering and terrorist financing risks. By having a fit for purpose EWRA, a firm would have adequately identified and assessed what products, services, transactions, customers or countries carry lower financial crime risks. As such, firms can utilise the outcomes of the EWRA to inform their SDD arrangements and controls.

In addition to determining whether the type of customer falls under any of the criteria set out in provisions 37(3)(a)&(b) of the MLR2017, firms are encouraged to consider the below factors when assessing whether a prospective relationship presents a low degree of risk and that the customer therefore, qualifies for SDD:

- The nature of a customer's business, or occupation for natural persons
- Whether the customer or individual has apparent substantial connections to high risk jurisdictions
- Whether there are substantial adverse media or concerns over the customer's or a beneficial owner's reputation/integrity
- Whether the customer's present a low level of risk but is seeking a higher risk product or service.

## SIMPLIFIED DUE DILIGENCE MEASURES

Firms are expected to utilise the outcomes of their customer risk assessments to dictate the level and extent of due diligence and ongoing monitoring. By the same token, firms must use the information gained/utilised to determine whether a customer qualifies for SDD, to decide on the level of SDD measures required.

A large number of firms often apply a uniform level of simplified measures to all low risk customers. By doing so, they may create slightly more efficient compliance processes, which are easier to follow by staff and their internal compliance functions. However, the Regulator expects firms to adjust the degree of due diligence in a way that is proportionate to the lower customer risks which were identified at the outset.

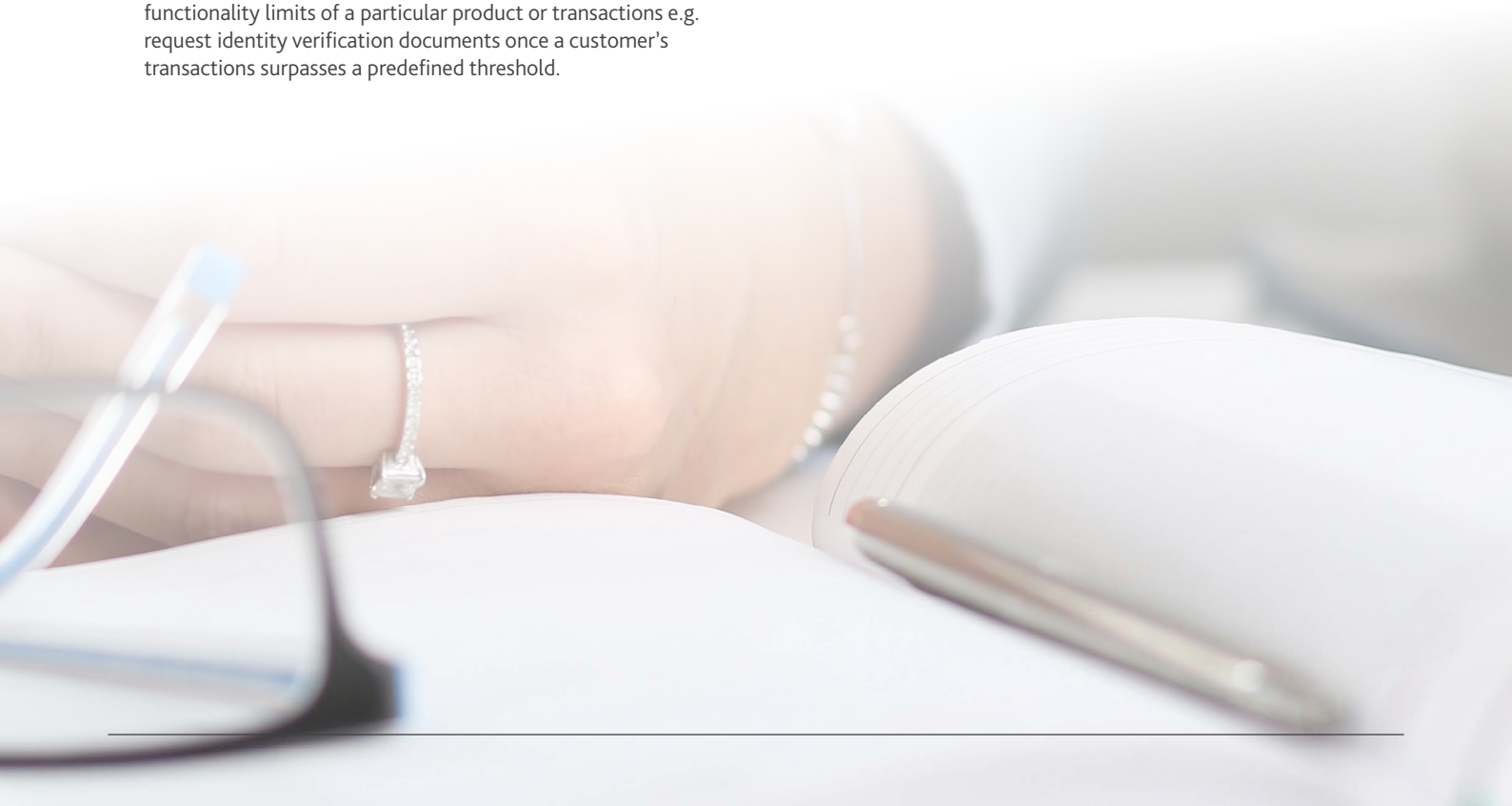
In applying risk-proportionate SDD measures, firms are encouraged to:

- Vary the amount and type of information required for verification purposes e.g. rely on fewer documents to verify the existence of a customer or use public information for verification purposes
- Identify the beneficial owner(s) of a customer without seeking additional information or documents to verify their identities
- Infer the purpose and nature of the proposed business relationship from the nature/type of both the client and the product or service sought
- Accept due diligence information directly from the customer as opposed to an independent source
- Hinge the amount of required CDD information on the functionality limits of a particular product or transactions e.g. request identity verification documents once a customer's transactions surpasses a predefined threshold.

It is critical for firms to consider the implication of applying simplified measures on their ongoing monitoring responsibilities. SDD does not exempt firms from conducting reviews of the business relationship. Similar to the standard due diligence measures, firms are expected to use the information gained when assessing the low levels of risk associated to particular customer, to:

- Ensure that they have sufficient knowledge about the customer, nature of the relationship and the customer's expected account activity to be able to identify unusual or suspicious activity
- Calibrate the frequency of CDD refreshes and periodic reviews
- Adjust the intensity and frequency of transaction monitoring.

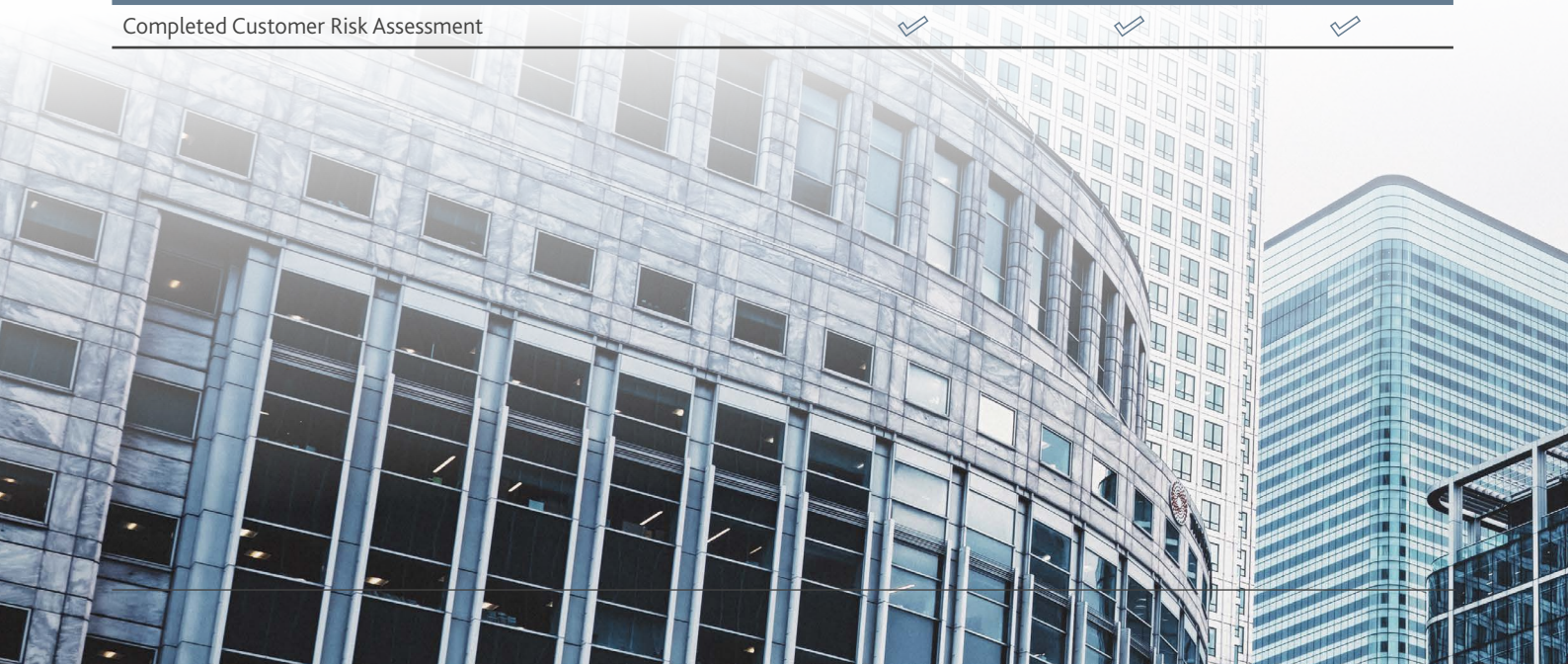
Whether or not firms have a large number of customers who carry lower risks and therefore qualify for SDD, it must always be kept in mind the application of SDD does not exempt a money laundering reporting officer from reporting suspicious activities to the competent authorities.



# SIMPLIFIED DUE DILIGENCE

## What does best practice look like?

| REQUIREMENT | SDD | CDD | EDD |
|---|---|---|---|
| **INFORMATION** | | | |
| Customer name | ✓ | ✓ | ✓ |
| Company/Registration number | ✓ | ✓ | ✓ |
| Country of Incorporation | ✓ | ✓ | ✓ |
| Registered Address | ✓ | ✓ | ✓ |
| Business/Correspondence Address (if applicable) | ✓ | ✓ | ✓ |
| Regulatory Status | ✓ | ✓ | ✓ |
| Listing Status | ✓ | ✓ | ✓ |
| Nature of Business | ✓ | ✓ | ✓ |
| Financial Information (turnover, assets, liabilities, etc.) | | ✓ | ✓ |
| Source of Wealth and Source of Funds | | ✓ | ✓ |
| Details of Directors | ✓ | ✓ | ✓ |
| Details of Signatories | ✓ | ✓ | ✓ |
| Details of Beneficial (25%) Owners | ✓ | ✓ | ✓ |
| Nature of Proposed Business Relationship/Type of Transactions | ✓ | ✓ | ✓ |
| Volume/Frequency of Transactions | ✓ | ✓ | ✓ |
| Estimated Value of Transactions | ✓ | ✓ | ✓ |
| **SCREENING** | | | |
| Entity PEP/Sanctions/Adverse Media Screening | ✓ | ✓ | ✓ |
| Directors PEP/Sanctions/Adverse Media Screening | ✓ | ✓ | ✓ |
| Beneficial Owners PEP/Sanctions/Adverse Media Screening | ✓ | ✓ | ✓ |
| **RISK ASSESSMENT** | | | |
| Completed Customer Risk Assessment | ✓ | ✓ | ✓ |



| REQUIREMENT | SDD | CDD | EDD |
|---|---|---|---|
| **DOCUMENTATION** | | | |
| Certificate of Incorporation | | ✓ | ✓ |
| Articles of Association | | ✓ | ✓ |
| Commercial Register Extract | | ✓ | ✓ |
| Proof of Business Address (where different to Registered Office) | | | |
| Proof of Regulation | ✓ | ✓ | ✓ |
| Proof of Listing | ✓ | ✓ | ✓ |
| Register of Directors | | ✓ | ✓ |
| Register of Shareholders | | ✓ | ✓ |
| Latest Audited Financial Statements | | ✓ | ✓ |
| Proof of Identity and Address for one or more Directors | | ✓ | ✓ |
| Proof of Identity and Address for all Beneficial (25%) Owners | | ✓ | ✓ |
| Source of Wealth and Source of Funds | | | ✓ |
| Proof of Identity and Address for Additional Directors | | | ✓ |
| Proof of Identity and Address for Additional Beneficial (e.g 10%) Owners | | | ✓ |
| Open Source Adverse Media Searches | | | ✓ |

**www.bdo.co.uk**

42001200